
Beyond the Privacy Calculus: Dynamics Behind Online Self-Disclosure



TECHNISCHE
UNIVERSITÄT
DARMSTADT

Department of Law and Economics
at the Technical University of Darmstadt

Doctoral thesis

by Amina Wagner

submitted in partial fulfilment of the requirements for the degree of
Doctor rerum politicarum (Dr. rer. pol.)

First assessor: Prof. Dr. Peter Buxmann
Second assessor: Prof. Dr. Alexander Benlian
Darmstadt 2021

Wagner, Amina

Beyond the Privacy Calculus: Dynamics Behind Online Self-Disclosure

written in Darmstadt, Germany, Technical University of Darmstadt, Department of Law and Economics, Software & Digital Business

in partial fulfillment of the Doctor rerum politicarum (Dr. rer. pol.)

Date of the viva voce: 06/14/2021

TUprints under CC BY-SA 4.0 International

<https://creativecommons.org/licenses/>

Declaration of Authorship

I hereby declare that the submitted thesis is my own work. All quotes, whether word by word or in my own words, have been marked as such.

The thesis has not been published anywhere else nor presented to any other examination board.

Ich erkläre hiermit ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig angefertigt habe. Sämtliche aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Die Arbeit wurde bisher weder einer anderen Prüfungsbehörde vorgelegt noch veröffentlicht.

Amina Wagner

Darmstadt, 7th April 2021

Abstract

Self-disclosure is ubiquitous in today's digitized world as Internet users are constantly sharing their personal information with other users and providers online, for example when communicating via social media or shopping online. Despite offering tremendous benefits (e.g., convenience, personalization, and other social rewards) to users, the act of self-disclosure also raises massive privacy concerns. In this regard, Internet users often feel they have lost control over their privacy because sophisticated technologies are monitoring, processing, and circulating their personal information in real-time. Thus, they are faced with the challenge of making intelligent privacy decisions about when, how, to whom, and to what extent they should divulge personal information. They feel the tension between being able to obtain benefits from online disclosure and wanting to protect their privacy. At the same time, firms rely on massive amounts of data divulged by their users to offer personalized services, perform data analytics, and pursue monetization.

Traditionally, privacy research has applied the privacy calculus model when studying self-disclosure decisions online. It assumes that self-disclosure (or, sometimes, usage) is a result of a rational privacy risk–benefit analysis. Even though the privacy calculus is a plausible model that has been validated in many cases, it does not reflect the complex nuances of privacy-related judgments against the background of real-life behavior, which sometimes leads to paradoxical research results. This thesis seeks to understand and disentangle the complex nuances of Internet users' privacy-related decision making to help firms designing data gathering processes, guide Internet users wishing to make sound privacy decisions given the background of their preferences, and lay the groundwork for future research in this field. Using six empirical studies and two literature reviews, this thesis presents additional factors that influence self-disclosure decisions beyond the well-established privacy risk–benefit analysis. All the studies have been published in peer-reviewed journals or conference proceedings. They focus on different contexts and are grouped into three parts accordingly: monetary valuation of privacy, biases in disclosure decisions, and social concerns when self-disclosing on social networking sites.

The first part deals with the value Internet users place on their information privacy as a proxy for their perceived privacy risks when confronted with a decision to self-disclose. A structured literature review reveals that users' monetary valuation of privacy is very context-dependent, which leads to scattered or occasionally even contradictory research results. A subsequent conjoint analysis supplemented by a qualitative pre-study shows that the amount of compensation, the type of data, and the origin of the platform are the major antecedents of Internet users' willingness to sell their data on data selling platforms. Additionally, an experimental survey study contrasts the value users ascribe to divulging personal information (benefits minus risks) with the value the provider gets from personal information. Building on equity theory, the extent to which providers monetize the data needs to be taken into account apart from a fair data handling process. In other words, firms cannot monetize their collected user

data indefinitely without compensating their users, because users might feel exploited and thus reject the service afterwards.

The second part delineates the behavioral and cognitive biases overriding the rational tradeoff between benefits and privacy risks that has traditionally been assumed in privacy research. In particular, evaluability bias and overconfidence are identified as moderators of the link between privacy risks and self-disclosure intentions. In single evaluation mode (i.e., no reference information available) and when they are overconfident, Internet users do not take their perceived privacy risks into account when facing a self-disclosure decision. By contrast, in joint evaluation mode of two information systems and when users are realistic about their privacy-related knowledge, the privacy risks that they perceive play a major role. This proof that mental shortcuts interact with privacy-related judgments adds to studies that question the rational assumption of the privacy calculus.

Moving beyond privacy risks, the third part examines the social factors influencing disclosure decisions. A structured literature review identifies privacy risks as the predominantly studied impediment to self-disclosure on social networking sites (SNS). However, a subsequent large scale survey study shows that on SNS, privacy risks play no role when users decide whether to self-disclose. It is rather the social aspects, such as the fear of receiving a negative evaluation from others, that inform disclosure decisions. Furthermore, based on a dyadic study among senders and receivers of messages on SNS, it is shown that senders are subject to a perspective-taking bias: They overestimate the hedonic and utilitarian value of their message for others. In this vein, these studies combine insights from social psychology literature with the uniqueness of online data disclosure and show that, beyond the potential misuse of personal information from providers, the risk of misperception in the eyes of other users is crucial when explaining self-disclosure decisions.

All in all, this thesis draws from different perspectives – including value measuring approaches, behavioral economics, and social psychology – to explain self-disclosure decisions. Specifically, it shows that the privacy calculus is oversimplified and, ultimately, needs to be extended with other factors like mental shortcuts and social concerns to portray Internet users' actual privacy decision making.

Abstract (German version)

Die Preisgabe persönlicher Informationen ist in der heutigen digitalisierten Welt allgegenwärtig, zum Beispiel bei der Kommunikation in Sozialen Medien oder beim Online-Shopping. Trotz der enormen Vorteile wie Bequemlichkeit, Personalisierung und anderer sozialer Belohnungen für dessen Nutzer¹, bringt dies massive Bedenken hinsichtlich der Privatsphäre mit sich. Darum äußern Internetnutzer die Sorge, dass sie die Kontrolle über ihre Privatsphäre verlieren, angeheizt durch ausgeklügelte Technologien, die persönliche Informationen überwachen, verarbeiten und in Echtzeit verbreiten können. Infolgedessen stehen Nutzer vor der Herausforderung, intelligente Entscheidungen darüber zu treffen, wann, wie, an wen und in welchem Umfang sie persönliche Informationen preisgeben. So sind sie mit dem Spannungsfeld zwischen der Möglichkeit, Vorteile aus der Nutzung von Online-Dienstleistungen zu ziehen, und der Notwendigkeit, ihre Privatsphäre zu schützen, konfrontiert. Gleichzeitig sind Unternehmen auf große Datenmengen angewiesen, um in der Lage zu sein, personalisierte Dienste anbieten, Datenanalysen durchführen oder persönliche Informationen für Werbezwecke monetarisieren zu können.

Traditionell hat die Datenschutzforschung bei der Untersuchung von Entscheidungen zur Informationspreisgabe im Internet das Modell des sogenannten „Privacy Calculus“ angewendet. Das Modell geht davon aus, dass die Selbstoffenbarung oder manchmal auch die Nutzung eines privatsphäreinvasiven Informationssystems das Ergebnis einer rationalen Risiko-Nutzen-Abwägung ist. Obwohl das Modell plausibel ist und in vielen Studien validiert wurde, spiegelt es nicht die komplexen Nuancen datenschutzbezogener Entscheidungen vor dem Hintergrund realer Verhaltensweisen wider, was manchmal zu unterschiedlichen oder sogar paradoxen Forschungsergebnissen führt. Ziel dieser Arbeit ist es daher, die komplexen Nuancen der Entscheidungsfindung von Internetnutzern in Bezug auf die Privatsphäre zu verstehen und zu entwirren. Dies unterstützt Unternehmen bei der Gestaltung ihrer Datenerfassungsprozesse, befähigt Internetnutzer vor dem Hintergrund ihrer Präferenzen, fundierte Privatsphäre-Entscheidungen treffen zu können und lenkt zukünftige Forschung in diesem Bereich.

In dieser Arbeit werden auf der Grundlage von sechs empirischen Studien und zwei strukturierten Literaturrecherchen Faktoren vorgestellt, die - über die etablierte Risiko-Nutzen-Analyse des Privacy Calculus hinaus - Entscheidungen zur Selbstoffenbarung beeinflussen. Alle Studien wurden von Fachleuten begutachtet und in Zeitschriften oder Konferenzbänden veröffentlicht. Sie beziehen sich auf unterschiedliche Kontexte und sind dementsprechend in drei Teile gegliedert: Monetäre Bewertung der Privatsphäre, Wahrnehmungsverzerrungen bei Entscheidungen zur Informationspreisgabe und soziale Bedenken bei der Selbstoffenbarung in Online Sozialen Netzwerken.

¹ Im Folgenden wird aus Gründen der besseren Lesbarkeit ausschließlich die männliche Form verwendet. Sie bezieht sich auf Personen beiderlei Geschlechts.

Der erste Teil beschäftigt sich mit dem Wert den Internetnutzer ihren persönlichen Informationen beimessen, stellvertretend für die Messung der wahrgenommenen Privatsphärerisiken bei der Preisgabe dieser Informationen. In einer Conjoint-Analyse, die durch eine qualitative Vorstudie ergänzt wird, wird gezeigt, dass die Höhe der Vergütung, die Art der Daten und die Herkunft der Plattform die wichtigsten Einflussfaktoren auf die Bereitschaft der Internetnutzer, ihre Daten auf Online-Datenmarktplätzen zu verkaufen, sind. Zusätzlich wird in einer experimentellen Befragungsstudie der Wert (Nutzen minus Risiken), den die Nutzer der Preisgabe von persönlichen Informationen zuschreiben, dem Wert, den der Anbieter aus den persönlichen Informationen gewinnt, gegenübergestellt. Aufbauend auf der „Equity“-Theorie muss neben einem fairen Umgang mit den Daten auch berücksichtigt werden, inwieweit die Anbieter die Daten monetarisieren. Mit anderen Worten: Unternehmen können ihre gesammelten Nutzerdaten nicht unbegrenzt monetarisieren, ohne ihre Nutzer zu entschädigen, denn die Nutzer könnten sich ausgenutzt fühlen und den Dienst aufgrund dessen ablehnen.

Im zweiten Teil werden Wahrnehmungsverzerrungen beschrieben, die die in der Privatsphäreforschung traditionell angenommene rationale Abwägung zwischen Nutzen und Datenschutzrisiken in Frage stellen. Insbesondere werden Wahrnehmungsverzerrungen, nämlich der sogenannte „Evaluability Bias“ und „Overconfidence Bias“, als Moderatoren des Zusammenhangs zwischen Privatsphärerisiken und Selbstoffenbarungsabsichten identifiziert. Im Modus der Einzelevaluierung (d.h. keine Referenzinformationen sind verfügbar) und bei Selbstüberschätzung in Bezug auf das eigene Datenschutzwissen berücksichtigen Internetnutzer ihre wahrgenommenen Privatsphärerisiken nicht, wenn sie mit einer Entscheidung zur Selbstoffenbarung konfrontiert werden. Im Gegensatz dazu spielen bei gemeinsamer Bewertung von zwei Informationssystemen und bei realistischer Einschätzung des datenschutzbezogenen Wissens der Nutzer die von ihnen wahrgenommenen Datenschutzrisiken eine große Rolle. Dieser Nachweis, dass Wahrnehmungsverzerrungen (Bias) mit datenschutzbezogenen Urteilen interagieren, ergänzt Studien, die die rationale Annahme des Privacy Calculus in Frage stellen.

Über die Risiken für die Privatsphäre hinaus befasst sich der dritte Teil mit sozialen Faktoren, die die Entscheidungen zur Offenlegung beeinflussen. Eine strukturierte Literaturrecherche identifiziert Risiken für die Privatsphäre als das überwiegend untersuchte Hindernis für die Selbstoffenbarung in Online Sozialen Netzwerken. Eine anschließende groß angelegte Umfragestudie zeigt jedoch, dass in diesen Netzwerken die Risiken für die Privatsphäre keine Rolle spielen, wenn Nutzer entscheiden, ob sie eigene persönliche Informationen preisgeben wollen. Vielmehr sind es die sozialen Aspekte, wie z.B. die Angst vor einer negativen Bewertung durch andere, die die Entscheidung beeinflussen. Des Weiteren wird anhand einer dyadischen Studie zwischen Sendern und Empfängern von Nachrichten auf Online Sozialen Netzwerken gezeigt, dass Sender einem sogenannten „Perspective-Taking Bias“ (Voreingenommenheit bei der Perspektiveneinnahme) unterliegen: Sie überschätzen den hedonistischen und utilitaristischen Wert ihrer Nachricht für andere. In diesem Sinne kombinieren diese Studien Erkenntnisse aus der sozialpsychologischen Literatur mit der Einzigartigkeit der Veröffentlichung von Daten im Internet und zeigen, dass neben dem potenziellen Missbrauch persönlicher Informationen von Anbietern auch das Risiko der Fehleinschätzung in den Augen anderer Nutzer ausschlaggebend für die Erklärung von Entscheidungen hinsichtlich der Preisgabe von eigenen persönlichen Daten ist.

Alles in allem greift diese Arbeit auf verschiedene Perspektiven zurück, wie z. B. Ansätze der Wertmessung, der Verhaltensökonomie und der Sozialpsychologie, um Entscheidungen zur Selbstoffenbarung zu erklären. Insbesondere zeigt diese Arbeit, dass der Privacy Calculus zu stark

vereinfacht ist und um weitere Faktoren wie Wahrnehmungsverzerrungen und soziale Bedenken erweitert werden muss, um die tatsächliche Entscheidungsfindung von Internetnutzern in Bezug auf den Schutz der Privatsphäre im Internet darzustellen.

Table of Contents

List of Figures	XII
List of Tables.....	XIII
List of Abbreviations.....	XIV
1 Introduction	1
Overarching Motivation	1
Overarching Research Questions and Contribution.....	2
Structure of the Thesis	5
2 Theoretical Background	8
Self-Disclosure	8
Information Privacy in the Digital Age.....	9
Beyond the Privacy Calculus	11
3 Research Paper 1.A: Value of Privacy.....	15
Introduction.....	16
Valuation of Privacy.....	17
Review Method	17
Integrative Framework	18
Discussion	23
Conclusion	25
4 Research Paper 1.B: Willingness to Sell Personal Information	26
Introduction.....	27
Related Work.....	29
Two-Step Study Design	30
Discussion	40
Limitations and Future Research Suggestions	41
Conclusion	42

5	Research Paper 1.C: Distributive Equity Perceptions of Data-Driven Services	43
	Introduction	44
	Theoretical Background on Users' Assessment of Free Data-Driven Service Providers	45
	Conceptual Model and Hypotheses Development	47
	Methodology of the Multi Study Approach	49
	Discussion	55
	Conclusion	60
6	Research Paper 2.A: Evaluability Bias in Privacy-Related Decisions	61
	Introduction	62
	Theoretical Background.....	63
	Research Method	68
	Results	71
	Discussion	75
	Limitations and Future Research Suggestions	78
	Conclusion	79
7	Research Paper 2.B: Overconfidence Bias in Privacy-Related Decisions.....	80
	Introduction	81
	Distortions in Privacy Decision Making	82
	Hypotheses Development and Research Model.....	84
	Method	86
	Results	88
	Discussion and Implications	91
	Limitations and Future Research Suggestions	93
	Conclusion	94
8	Research Paper 3.A: Antecedents of Self-Disclosure on SNS.....	95
	Introduction	96
	Review Method	96
	Results	97
	Discussion	103
	Conclusion, Limitations and Future Research Suggestions	103

9	Research Paper 3.B: From Privacy Calculus to Social Calculus	105
	Introduction	106
	Theoretical Background	107
	Qualitative Pre-Study: Self- vs. Other-Focus	109
	Hypotheses Development and Research Model	112
	Quantitative Main Study	115
	Results	116
	Discussion	118
	Limitations and Future Research Suggestions	120
	Conclusion	120
10	Research Paper 3.C: Perspective-taking Bias on SNS	121
	Introduction	122
	Conceptual Background and Hypotheses Development	123
	Research Method	127
	Results	130
	Discussion	132
	Limitations and Future Research Suggestions	134
	Conclusion	135
11	Overarching Findings and Discussion	136
12	Concluding Remarks	142
	References	143
	Appendix	177

List of Figures

Figure 1. Biases in privacy-related judgements.	12
Figure 2. Integrative theoretical framework of valuation of privacy.	19
Figure 3. Overview of the two-step study.	31
Figure 4. Conceptual model.	47
Figure 5. Multi-study approach.	50
Figure 6. Screenshot of the Facebook web app.	52
Figure 7. Results of the PLS analysis.	55
Figure 8. Research model.	66
Figure 9. App store screenshots (translated to English), left: application A, right: application B.	69
Figure 10. Conceptual research model.	84
Figure 11. Conceptual research model.	112
Figure 12. Research model with path coefficients and significance levels.	118
Figure 13. Sender-recipient relationship on SNSs.	124
Figure 14. Perceptual congruence model of the shared content value.	126
Figure 15. Research model on the effects of sender's understanding of the recipient.	127
Figure 16. Perceptual congruence scoring table (Benlian and Haffke 2015).	129
Figure 17. Mean values reported by senders and recipients (H1).	131
Figure 18. Congruence scores on actual agreement vs. perceived agreement (H2).	131
Figure 19. Results of the structural model testing (**p<0.001, *p<0.01).	132
Figure 21. Extension of the privacy calculus model with additional factors.	137

List of Tables

Table 1. List of publications included in this thesis.....	5
Table 2. Outline of research papers.....	6
Table 3. Studies on SNS users' valuation of their profile information.	10
Table 4. Articles on mental shortcuts in privacy-related judgements.	12
Table 5. SNS artifacts.	14
Table 6. Antecedents of users' WTS personal information on data-selling platforms.	32
Table 7. Summary of attributes and attribute levels of the CBC study.	36
Table 8. Attributes, levels, part-worths, and average importancia.	39
Table 9. Utility changes and monetary value of changes.....	39
Table 10. Demographic information of main study's respondents.	53
Table 11. Mean, Standard Deviation (SD), Cronbach's α (Cr. α), Composite Reliability (CR), Average Variance Extracted (AVE) and Construct correlations.	54
Table 12. Item loadings and item reliabilities.....	73
Table 13. Cronbach's α (Cr. α), Composite Reliability (CR), Average Variance Extracted (AVE) and Construct correlations (single evaluation sample in first lines and joint evaluation sample in second lines).....	73
Table 14. Results of structural model testing.....	74
Table 15. Survey items and item loadings (OC=overconfident; NOC=non-overconfident).	89
Table 16. Cronbach's α (Cr. α), Composite Reliability (CR), Average Variance Extracted (AVE) and Construct correlations (overconfident in the first and non-overconfident in the second row).	90
Table 17. Effect sizes and results of structural model testing (** $p < 0.001$; ** $p < 0.01$; * $p < 0.05$).....	91
Table 18. Results of t-tests.	91
Table 19. Theoretical frameworks used to study self-disclosure.	97
Table 20. Benefits of self-disclosure.	99
Table 21. Costs of self-disclosure and cost-mitigating factors.	100
Table 22. Personality factors and their relation to self-disclosure.	102
Table 23. Summary of pre-study results.	111
Table 24. Construct validity measures.....	117
Table 25. Explanation of perceptual congruence measures (S- Sender; R- Recipient).....	125

List of Abbreviations

App	Application
AVE	Average Variance Extracted
BDM	Becker-DeGroot-Marshak Mechanism
CA	Conjoint Analysis
CBC	Choice-Based Conjoint
CR	Composite Reliability
Cr. α	Cronbach's Alpha
CVM	Contingent Valuation Method
DCM	Discrete Choice Method
FtF	Face-to-Face
H	Hypothesis
IS	Information Systems
JE	Joint Evaluation
M	Mean
NOC	Non-Overconfident
OC	Overconfident
Q	Question
R	Recipient
RQ	Research Question
S	Sender
SD	Standard Deviation
SE	Single Evaluation
SNS	Social Networking Sites
VHB	Verband der Hochschullehrer für Betriebswirtschaft e.V.
VA	Vickrey Auction
WTA	Willingness to Accept
WTP	Willingness to Pay
WTS	Willingness to Sell

1 Introduction

Online self-disclosure currently forms the backbone of information technologies (Boyd and Heer 2006) that process, aggregate, and monetize large amounts of user data to be able to offer personalized services or invent new ones. At the same time, it requires Internet users to manage their privacy preferences with asynchronous feedback cycles, constantly changing technological affordances, and associated threats to privacy (Choi and Bazarova 2020; Dinev 2014; Smith et al. 2011). Therefore, this thesis revolves around the dynamics behind online self-disclosure decisions, their antecedents and situational factors, as well as cognitive and social dilemmas.

Overarching Motivation

Defined as “any message about the self that a person communicates to another” (Wheless and Grotz, 1976, p. 338), self-disclosure is a common act online. It happens when Internet users reveal personal information that was previously private and unknown to either organizations or other individuals (Laufer and Wolfe 1977). Online self-disclosure has become ubiquitous, with 2.7 billion meeting minutes in Microsoft Teams per day (Spataro 2020), 40,000 searches on Google every second (Internet live Stats 2020), and 500 million stories shared daily on Instagram alone (Statista 2020a). Self-disclosure is even higher online than in offline communication (Tidwell and Walther 2002) because it is a prerequisite to reduce uncertainty and build intimacy (Park et al. 2011). People are turning to digital technologies to maintain friendships or to share news (Anderson and Vogels 2020) – even more so at the time of this writing amid the COVID-19 pandemic.

A key recurring scheme to explain Internet users’ online self-disclosure is a normative theory that describes self-disclosure as a result of a cost–benefit analysis (Li 2012; Smith et al. 2011). On the benefit side, users release their personal information in exchange for monetary rewards (Preibusch 2015), personalization (Chelappa and Sin 2005), and other social benefits (Krasnova et al. 2010a). On the cost side, a privacy calculus lens has traditionally been applied, which defines privacy risks as the major impediment to self-disclosure (Dinev and Hart 2006; Laufer and Wolfe 1977). Thus, according to the privacy calculus, individuals self-disclose if they perceive the benefits to be greater than the privacy risks (Culnan and Armstrong 1999; Dinev and Hart 2006; Krasnova et al. 2010a). It implies that individuals act as rational agents on the basis of all relevant information and ultimately make deliberate decisions (Adjerid et al. 2018). However, pioneering studies have started to question this normative assumption because the research findings building on the privacy calculus are not consistent across contexts (John et al. 2011), which challenges the notion of stable privacy preferences. Dinev et al. (2015) explains these paradoxical research results by pointing to situational factors like affect, incomplete information, or mental shortcuts that distort rational decision making. Especially when comparing individuals’ privacy preferences with their actual behavior, the limited explicability of actual self-disclosure behavior by the rational tradeoff between benefits and privacy risks becomes salient (Alashoor and

Baskerville 2015). This phenomenon is also known as the privacy paradox and describes an inconsistency between users' stated perceptions and their actual act of self-disclosure (Adjerid et al. 2018; Norberg et al. 2007; Wilson and Valacich 2012).

Indeed, poll after poll has shown that individuals' privacy concerns are on the rise, with 81 percent of respondents stating that "potential risks of companies collecting data about them outweighs the benefits" (Pew Research 2019). Except for health care, it is the biggest concern among U.S. population (Wunderman Thompson 2020). At the same time, however, many Internet users self-disclose personal information on social networking sites, reveal their shopping information by using loyalty cards, and give smartphone application providers access to their personal information like contacts and photos. Even after a privacy breach like Cambridge Analytica, only 6 percent say they will definitely delete their Facebook account because of it (Statista 2020b). Against the background of paradoxical observations and situation-specific decisions, the privacy calculus seems to be oversimplified when explaining actual disclosure behavior (Dinev et al. 2015). Emphasizing a simple tradeoff between privacy risks and benefits, prior research lacks comprehensive descriptions of the context-dependent factors that drive or inhibit self-disclosure online.

In an attempt to dig deeper into Internet users' disclosure, this thesis seeks to identify further nuances of their self-disclosure decision making beyond the well-established privacy calculus. Since self-disclosure is almost impossible without giving up some measure of privacy, investigating the role of perceived privacy risks is the main focus of this work. Given the ubiquitous nature of self-disclosure in today's digitized society, along with rising privacy issues like online behavior tracking, identity theft, and third-party usage of personal information, the phenomenon of online self-disclosure is highly discussed in media, research, and society. On the one hand, it is of great interest to online companies because their business models rely on massive amounts of user data to provide services and, ultimately, gain revenue. On the other hand, users enable these products by releasing their personal information to firms, and ultimately pay with their privacy which, in turn, put their privacy at risk. Internet users are faced with the challenge of deciding what, when, and to what extent they should divulge their personal information online. Additionally, protecting users' privacy online has become an important topic for policymakers as well and recently resulted in the General Data Protection Regulation (GDPR) in the EU.

Overall, understanding the underlying dynamics of privacy-related judgments is one of the key concerns of the information age (Bélanger and Crossler 2011). In this vein, this thesis contributes knowledge to firms relying on a constant release of data, users seeking to make intelligent privacy choices, and scientists trying to explain inconsistencies across previous studies and actual privacy-related decisions.

Overarching Research Questions and Contribution

Motivated by the lack of empirical explanations for the complex nuances behind self-disclosure decision making, this thesis tackles this research gap from three perspectives. First, because Internet users trade their personal information for digital services, the value of privacy from a user perspective is assessed. The value Internet users place on their personal information serves as a proxy for the risk-benefit analysis manifested in the privacy calculus. Based on a literature review (Paper 1.A), we find that studies building on the monetary valuation of privacy found very low and inconsistent amounts. While Schreiner and Hess (2015) showed that study participants would pay 0.63 euros per month for a premium version of Facebook, Krasnova et al.'s (2009a)

conjoint analysis found respondents would pay monthly fees of 1.20 and 1.40 euros for a privacy-enhanced SNS. Overall, these scattered results highlight that self-disclosure decisions are very context-sensitive. This is especially problematic for data-driven business providers that rely on their users constantly releasing data. As yet, they cannot make predictions by using current research where users refrain from sharing information due to the high risk to their privacy or when privacy plays only a minor role. A more neutral and realistic study design is missing to measure individuals' value of personal information with fewer situational influences. Therefore, this thesis adds to the literature stream on the value of personal information by investigating the relative importance of the antecedents of individuals' willingness to sell their information based on a choice-based conjoint analysis together with the benefits of a qualitative pre-study.

Additionally, IS privacy research has been predominantly focused on the value of privacy for users. Specifically, prior research building on the privacy calculus has defined privacy-related decisions as the result of an intrapersonal benefit-risk analysis (Li 2012). In this regard, Internet users are assumed to only balance their own benefits and privacy risks when confronted with a self-disclosure decision. By building on equity theory (Adams 1965; Leventhal 1980), this intrapersonal analysis is extended by interpersonal factors. Equity theory suggests that, in a social exchange relationship including customers and providers, customers incorporate the net value of the provider into their decision-making process (Oliver and Swan, 1989). In this vein, the value of the provider is the basis of their own deservingness, which is contrasted with their net value (benefits minus risks) (Martinez-Tur et al. 2006). If the provider's net value is higher than their own, values are unfairly distributed, which leads to a feeling of exploitation (Oliver and Swan, 1989). This should be of great interest to data-driven business providers because they have to monitor how their value from personal information is perceived in order to avoid a feeling of unfairness, which could lead them to reject the service. Therefore, this thesis adds to privacy research by investigating how much the net value from personal information informs Internet users' attitudes to those providers and whether it further affects satisfaction and their intention to continue using the service. Investigating the value that Internet users assign to their privacy and its relation to providers' value from monetizing personal information is reflected in the first overarching research question:

RQ1: What influences the value Internet users assign to their privacy? And how does it relate to providers' value from personal information?

Secondly, explanations are sought for irrational privacy choices in light of the privacy calculus. While some studies have found a significant negative link between privacy risks and self-disclosure (Keith et al. 2013; Krasnova et al. 2010a), others have found a minor relationship (Acquisti and Gross 2006; Shibchurn and Yan 2015) or even no significant effect at all (Cheung et al. 2015). For instance, Krasnova et al. (2010a) found evidence of the privacy risk-intention relationship. They point to privacy risks as the major impediment to self-disclosure on SNS. By contrast, Brakemeier et al. (2016) show that SNS users' disposition toward privacy risks depends on their current focus on prevention or promotion. Similarly, optimism bias, endowment, and order effect have been identified as biases that distort stable self-disclosure decision making across contexts (Acquisti et al. 2009; Acquisti and Grossklags 2005a; Baek et al. 2014). Literature questioning the linear link between privacy risks and self-disclosure builds on knowledge from behavioral economics because it argues that decision making deviates from rationality (Tversky and Kahneman 1973) due to immediate gratification, bounded rationality, and incomplete information (Acquisti 2004) when people have to make disclosure decisions. Still, knowledge about the behavioral and cognitive biases in self-disclosure decisions is underdeveloped.

Therefore, this thesis tests how evaluability and overconfidence bias interact with disclosure behavior. In extant research to date, privacy risks have been measured as the magnitude to which Internet users are concerned about data protection. However, what has been overlooked is in how far users are confident in their risk assessments. The evaluability bias tests how confidence varies depending on available reference information and the overconfidence bias examines the effect of unrealistically high confidence on privacy assessments. Both biases may help explain why privacy risks are not always significantly linked to disclosure behavior in prior research. Privacy-friendly firms can use this knowledge to educate their users in terms of privacy to make privacy-friendliness a competitive advantage. The extension of the privacy calculus with cognitive and behavioral biases is delineated in the second overarching research question:

RQ2: How do evaluability bias and overconfidence influence privacy-related judgements of online companies?

Thirdly, social concerns are identified as an underexplored impediment of online self-disclosure. Beyond privacy concerns, research has shown that Internet users refrain from sharing personal information because their information can be misunderstood (Min 2016) or their relationships might suffer (Yu et al. 2015). Specifically, in the context of online communication, users of SNS have been shown to think strategically about their postings by specifically targeting their audience (Barasch and Berger 2014) or using filters (Hu et al. 2014). On social media, 43 percent of U.S. teens feel pressure to only post things that make them look good (Anderson and Jiang 2018). Nevertheless, the price of sharing is commonly described as privacy risks focusing on data protection from organizational threats, which is rooted in the e-commerce context where personal information is traded to gain certain benefits in return (Dinev and Hart 2006). However, on SNS, users are voluntarily disclosing information to communicate with others (Kane et al. 2014). Apart from personal information such as their name, address, and telephone number, SNS users are expressing their thoughts, experiences, and daily lives to get feedback from others (Utz 2015). Rather than just transferring data, this disclosure of information goes beyond the concerns of data protection and security. It implies a social component that incorporates the perception of intended others to maintain relationships or construct an identity in the eyes of others (Yu et al. 2015; Zhao et al. 2008), but scholars have paid considerably less attention to social concerns and their influence on the decision to self-disclose. This thesis aims to close the gap and help SNS providers by providing an additional explanation for why their users refrain from sharing personal information, which may cause a competitive disadvantage and, in turn, severe financial problems. A subsequent dyadic study of senders and recipients of messages tests whether those social concerns are justified. In this regard, an assessment based on empathy theory determines whether those who send the information correctly anticipate their recipients' perceptions and reactions. If not, they are subject to a perspective-taking bias. SNS users can learn from these results by realistically accounting for the perceptions of their information recipients while still realizing the benefits of self-disclosure. This leads us to the third and final overarching research question:

RQ3: Do social concerns impact Internet users' self-disclosure decisions? And if so, are they subject to a perspective-taking bias?

To sum up, this thesis makes three attempts: (1) It measures the value of privacy along with its antecedents and in relation to providers' net value from personal information, (2) it investigates mental shortcuts that distort the linear link between privacy risks and self-disclosure, and (3) it identifies worries beyond the privacy concerns (i.e., social concerns) of SNS users and their effect on self-disclosure decisions as well as interpersonal dilemmas.

Structure of the Thesis

Guided by these three research questions, the thesis encompasses eight research essays published in peer-reviewed outlets ranging from conference proceedings to journal articles and listed in Table 1. In response to RQ1, Papers 1.A, 1.B, and 1.C tackle the value of privacy from a user perspective. Starting with an extensive literature review, the first paper develops a comprehensive framework that presents studies measuring the value of personal information. This literature review forms the basis for the two corresponding empirical studies. First (Paper 1.B), with the help of a conjoint analysis, antecedents of Internet users' willingness to sell their personal information on data-selling platforms and their relative importance are provided. And second (Paper 1.C), users' perception of providers' value gained from personal information is manipulated, and its impact on distributive equity perceptions is investigated. Papers 2.A and 2.B are concerned with deviations from rational privacy judgments and, therefore, respond to RQ2. The main premise of the two tested models is to identify the cognitive biases that moderate the link between privacy risks and self-disclosure intentions. Continuing with RQ3, Paper 3.A presents a second structured literature review, which results in a comprehensive list of antecedents of self-disclosure in the SNS context. Extending this research stream on SNS users' self-disclosure, Paper 3.B classifies social concerns as an overlooked impediment to releasing personal information online. Also not free from cognitive distortions, social perceptions online are shown to be subject to a perspective-taking bias in Paper 3.C.

Table 1. List of publications included in this thesis.

RQ1	Paper 1.A	Wagner, Amina; Wessels, Nora; Buxmann, Peter; Krasnova, Hanna (2018): Putting a Price Tag on Personal Information - A Literature Review . In: Hawaii International Conference on System Sciences (HICSS), Waikoloa Village, Hawaii, VHB-Ranking: C.
	Paper 1.B	Wessels, Nora; Gerlach, Jin P.; Wagner, Amina (2019): To Sell or not to Sell – Antecedents of Individuals' Willingness-to-Sell Personal Information on Data-Selling Platforms . In: International Conference on Information Systems (ICIS), Munich, Germany, VHB-Ranking: A.
	Paper 1.C	Wagner, Amina; Wessels, Nora; Brakemeier, Hendrik; Buxmann, Peter (2021): Why Free Does not Mean Fair: Investigating Distributive Equity Perceptions of Data-Driven Services . In: International Journal of Information Management (59), VHB-Ranking: C.
RQ2	Paper 2.A	Brakemeier, Hendrik; Wagner, Amina; Buxmann, Peter (2017): When Risk Perceptions Are Nothing but Guesses – An Evaluability Perspective on Privacy Risks . In: International Conference on Information Systems (ICIS), Seoul, South Korea. VHB-Ranking: A.
	Paper 2.B	Wagner, Amina; Mesbah, Neda (2019): Too Confident to Care: Investigating Overconfidence in Privacy Decision Making . In: European Conference on Information Systems (ECIS), Stockholm, Sweden, VHB-Ranking: B.
RQ3	Paper 3.A	Abramova, Olga; Wagner, Amina; Krasnova, Hanna; Buxmann, Peter (2017): Understanding Self-Disclosure on Social Networking Sites - A Literature Review . In: Americas Conference on Information Systems (AMCIS), Boston, USA, VHB-Ranking: D.

Paper 3.B	Wagner, Amina; Krasnova, Hanna; Abramova, Olga; Buxmann, Peter; Benbasat, Izak (2018): From Privacy Calculus' to 'Social Calculus': Understanding Self-Disclosure on Social Networking Sites. In: International Conference on Information Systems (ICIS), San Francisco, USA, VHB-Ranking: A.
Paper 3.C	Wagner, Amina; Abramova, Olga; Krasnova, Hanna; Buxmann, Peter (2018): When You Share, You Should Care: Examining the Role of Perspective-Taking on Social Networking Sites. In: European Conference on Information Systems (ECIS), Portsmouth, UK, VHB-Ranking: B.

A variety of research designs are employed in the eight publications included in this thesis (see Table 2, column 2). Apart from structured literature reviews in papers 1.A and 3.A, a conjoint analysis, as well as qualitative and quantitative studies, was conducted. By taking advantage of the exploratory nature of qualitative studies (Mingers 2001; Venkatesh et al. 2013), they are used as pre-studies to dig deeper into Internet user's perceptions or behavioral motivations. In particular, a qualitative research design with the help of an open-ended online survey was conducted in Paper 3.B. Paper 1.B makes use of in-depth interviews. Both studies were done to complement the follow-up quantitative studies and, thus, provide a more substantive reasoning for users' actual behavior. Quantitative research designs have been applied based on empirical online surveys in papers 1.C, 2.A, 2.B, 3.B, and 3.C. Some of them use a quasi-experimental design by presenting respondents with differing scenarios. A choice-based conjoint analysis was employed in Paper 1.B to measure the respondents' willingness to sell their personal information.

Table 2. Outline of research papers.

Chapter and Research Paper	Research Type and Methodology	Theoretical Background	Context
Chapter 3 Research Paper 1.A: Value of Privacy	Structured Literature Review	Valuation of Privacy	Multitude
Chapter 4 Research Paper 1.B: Willingness to Sell Personal Information	Qualitative Pre-Study Conjoint Analysis	Valuation of Privacy	Data-selling Platforms
Chapter 5 Research Paper 1.C: Distributive Equity Perceptions of Data-Driven Services	Construct Validity Assessment Experimental Survey Study	Privacy Calculus Distributive Equity Theory	Data-driven Service Providers
Chapter 6 Research Paper 2.A: Evaluability Bias in Privacy-Related Decisions	Experimental Survey Study	Privacy Calculus Behavioral Economics (Evaluability Theory)	Mobile Applications
Chapter 7 Research Paper 2.B: Overconfidence Bias in Privacy-Related Decisions	Experimental Survey Study	Privacy Calculus Behavioral Economics (Overconfidence)	Mobile Applications

Chapter 8 Research Paper 3.A: Antecedents of Self-Disclosure on SNS	Structured Literature Review	Self-disclosure on Social Networking Sites	Social Networking Sites
Chapter 9 Research Paper 3.B: From Privacy Calculus to Social Calculus	Qualitative Pre-study Survey Study	Privacy Calculus Interpersonal Communication Theory Impression Management	Social Networking Sites
Chapter 10 Research Paper 3.C: Perspective-Taking Bias on SNS	Dyadic Study	Empathy Theory (Perspective-Taking Literature)	Social Networking Sites

In addition to the publications included in this cumulative dissertation (see Table 1), I co-authored the following peer-reviewed publications during my time as a Ph.D. candidate at the Technical University of Darmstadt, Germany:

- Wagner, Amina; Olt, Christian M.; Abramova, Olga (2021): Calculating versus Herding in the Adoption and Continuance Use of a Privacy-Invasive Information System: The Case of COVID-19 Tracing Apps. In: European Conference on Information Systems (ECIS), Marrakesh, Morocco, VHB-Ranking: B.
- Olt, Christian M.; Wagner, Amina (2020): Having Two Conflicting Goals in Mind: The Tension Between IS Security and Privacy when Avoiding Threats. In: Hawaii International Conference on System Sciences (HICSS), Wailea, USA, VHB-Ranking: C.
- Krause, Hannes-Vincent; Wagner, Amina; Krasnova, Hanna; große Deters, Fenne; Baumann, Annika; Buxmann, Peter (2019): Keeping Up with the Joneses: Instagram Use and its Influence on Conspicuous Consumption. In: International Conference on Information Systems (ICIS), Munich, Germany, VHB-Ranking: A.
- Wessels, Nora; Wagner, Amina; Prakash Sarswat, Jayesh; Buxmann, Peter (2019): What is Your Selfie Worth? A Field Study on Individuals' Valuation of Personal Data. In: Internationale Tagung Wirtschaftsinformatik (WI), Siegen, Germany, VHB-Ranking: C.
- Wagner, Amina; Gasche, Lisa Alina (2018): Sharenting: Making Decisions About Other's Privacy on Social Networking Sites. In: Multikonferenz Wirtschaftsinformatik (MKWI), Lüneburg, Germany, VHB-Ranking: D.

All publications included in this thesis² appear in Chapter 3 to 10. In Chapter 2, the overarching theoretical fundamentals of the thesis are defined. The work concludes with an overarching discussion of all the studies' results in Chapter 11, as well as suggestions for future research and final remarks in Chapter 12.

² The papers have been slightly adapted from their original versions to have a consistent layout throughout this thesis. Additionally, they are written from the first-person plural (i.e., "we") perspective, since co-authors contributed to every publication.

2 Theoretical Background

This chapter explains overarching concepts that are investigated in the research papers forming this cumulative thesis. Specifically, it presents the term self-disclosure, information privacy, and its measurements and conceptualizations. Finally, this chapter closes with an introduction to factors affecting disclosure decisions beyond the privacy calculus.

Self-Disclosure

Self-disclosure is defined as any information that is released from one person to another (Wheeless and Grotz 1976). In general, it is characterized by its depth, breadth and duration (Taylor and Altman 1975). Depth describes the intimacy of the disclosiveness, whereas breadth revolves around its variety of topics, and duration deals with the frequency and time spent to disclose the information (Omarzu 2000; Wheelless and Grotz 1976). On the one hand, Internet users disclose information voluntarily (Smith et al. 2011) in order to maintain relationships, transact with a provider or by broadcasting themselves. To be more explicit, users share private or public messages as well as release their names, addresses and bank details to online providers in order to use certain services. On the other hand, information is rather involuntarily shared by reading a news website or using search engines. Thereby, website providers can trace users' online behavior, IP-addresses, and other related personal information that can be used for personalization or advertisement purposes (Culnan and Bies 2003).

As such, self-disclosure online differs compared to face-to-face communication since information is easily searchable, stored and shared (Boyd and Ellison 2008). Additionally, it is an important prerequisite for online organizations because self-disclosure leverages personalized services and provides real-time customer insights (Xu et al. 2009). Therefore, research in Information Systems (IS) has investigated the extent (Hollenbaugh and Ferris 2015), antecedents (Cheung et al. 2015; Krasnova et al. 2010a; Wirth et al. 2019), and outcomes of self-disclosure such as life satisfaction (Jiang et al. 2011; Krasnova et al. 2015). With a rising share, research is predominantly looking at the extent of self-disclosure to other users on SNS and its providers. For instance, Acquisti and Gross (2006) show that 84 percent of Facebook users reveal their real names on SNS. In a similar vein, others have found evidence that SNS users share more intimate and truthful information to friends than to strangers online (Utz 2015).

Even though investigating the online self-disclosure phenomenon is heightened, its measurement varies. Word counting, content analysis, and self-reported measures have been applied to capture past self-disclosure behavior (Joinson and Paine 2007). In an attempt to measure the intention to self-disclose, a great number of researchers have relied on individuals' likelihood to reveal a certain piece of information (e.g., Krasnova et al. 2010a; Zhao et al. 2012), or individuals' likelihood to use an information system as a proxy (Brakemeier et al. 2016b). Actual self-disclosure is assessed based on laboratory (e.g., Cvrcek et al. 2006; Tsai et al. 2011) or field experiments (Acquisti et al. 2009). For instance, Acquisti et al. (2009) tested in a field study in

how far customers disclose their personal information by using a loyalty card in exchange for monetary discounts.

Information Privacy in the Digital Age

When releasing personal information online, people give up some extent of their information privacy. Therefore, privacy evolved as an important concept when studying self-disclosure online (Joinson et al. 2007; Trepte et al. 2020). In essence, privacy is defined as the right to be left alone (for review see Warren and Brandeis 2015). With the rise of digital technologies that gather, store and process large amounts of personal information, a sub concept termed information privacy emerged (Smith et al. 2011). However, the definition of information privacy remains mixed in terms of its conceptualization, measurements, and its distinction from other constructs (Pavlou 2011). Two definitions evolved into the most established ones in IS research: privacy as control and privacy as commodity.

The control-based definition of privacy refers to users' wish of autonomy about how, when, and to what extent data is shared. Since personal information can be searched, stored and processed in an unforeseen way without the consensus of the user, users worry about losing control over their personal information (Bélanger and Crossler 2011; Malhotra et al. 2004). According to Smith et al. (1996), this worry relates to four subcategories: awareness of privacy practices, avoidance of errors, unauthorized secondary data use, and improper access. It is commonly measured as Internet users' perception of data handling processes (Dinev and Hart 2006; Malhotra et al. 2004).

The commodity based definition refers to the fact that users trade their personal information like an intangible asset in exchange for service benefits, for example personalization (Xu et al. 2009) or social rewards (Ellison et al. 2007; Krasnova et al. 2010a). This definition is particularly salient in information privacy research. On the one hand, because Internet users constantly release their personal information in order to receive benefits from free data-driven online services. On the other hand, because data-driven online companies monetize their customers' data by providing advertisement services to third parties, adding value to their own services or reduce transaction costs (Aïmeur et al. 2016) based on the released information by users. In this regard, the average revenue per user for Facebook and Google alone reached \$59 in 2017 (European Union Agency for Cybersecurity 2018) which demonstrates the tremendous value of personal information. "Thus, a tension exists between the users' desire to protect personal data and the need of Internet retailers for consumer information that drives the customer relationship process to understand preferences, meet needs, customize products and services, and market new opportunities – activities that benefit both the user and the organization." (Wakefield 2013, p. 157-158). Therefore, assigning values to personal information from a user perspective helps firms to account for the users' wish to protect ones' privacy or the amount that needs to be offered as a form of compensation for releasing personal information.

Valuation of Privacy

Taking into account the tremendous value of user data for companies, exemplified by the stock value of data-driven business models (Eling et al. 2016), the value users' place on their personal information has been examined. Under the umbrella of economics of privacy (Brandimarte and Acquisti 2012), Acquisti et al. (2013) have asked the question "What is privacy worth?". However, their study resulted in no clear value attributed to privacy from a user perspective. It is dependent on whether users are asked to sell a certain type of information or how much they would pay to protect it (Acquisti et al. 2013). Similarly, others provided evidence that valuation of privacy

depends on situational factors such as the purpose of data collection (Danezis et al. 2005), the collecting organization (Nguyen et al. 2016), as well as the study design (Benndorf and Normann 2014). Thus, the question “What is privacy worth?” is very context sensitive. Beyond putting a value on personal information, scholars asked the question of whether Internet users value their personal information at all (Acquisti 2004; Preibusch et al. 2013), because of their unstable preferences. Indeed, research has provided evidence that Internet users voluntarily release their personal information for minor benefits (Grossklags and Acquisti 2007). For instance, Cvrcek et al. (2006) found that users would sell their location data for the price of a burger while Bauer et al. (2012) provided evidence that 48 percent of their study participants would not pay a Cent to prevent their Facebook data from deletion.

Concluding from these results, studies investigating to what extent users value their personal information are scattered. Table 3 below presents studies measuring the value users place on their SNS profile information and its deviating results. For instance, the study from Krasnova et al. (2009b) resulted in a yearly fee of 14.14 to 17.24 euros for a premium version of Facebook without advertisement while Schreiner and Hess (2015) study yield 50 percent less.

Table 3. Studies on SNS users' valuation of their profile information.

Type of Personal Information	Value of Personal Information	Articles
Demographic Information on Facebook	Respondents would pay on average between 14.14 and 17.24 euros as a yearly fee for an SNS without advertisement.	Krasnova et al. (2009b)
Facebook Profile Information	Respondents would pay on average 9.45 euros to save their profile from deletion.	Bauer et al. (2012)
Facebook Profile Information	Respondents who were willing to sell their profile information requested on average 19 euros.	Benndorf and Normann (2014)
Facebook Profile Information	Respondents would pay on average 0.63 euros for a premium version of Facebook per month.	Schreiner and Hess (2015)

At the same time, however, Internet users state high privacy concerns and abandon companies which are not trusted (Jensen et al. 2005) or put their data at risk (Culnan 1993). Similarly, users find it unfair that their personal data is extensively monetized by online companies (Aïmeur et al. 2016; Culnan and Bies 2003). In this vein, data selling platforms (e.g., DataCoup) have emerged where users can actively monetize their data by selling it to third parties (Spiekermann et al. 2015a, 2015b). However, these data-selling platforms have not yet reached a high user rate due to ethical issues and low monetary incentives.

Privacy Calculus

Considering the ubiquitous nature of the self-disclosure phenomenon and heightened privacy concerns, research investigating the determinants of disclosure decisions is omnipresent (e.g., Chang and Heo 2014). For example, boyd and Ellison (2008) showed that SNS users regularly share status updates in order to gain social capital. Another study by Chelappa and Sin (2005), provided evidence that users share their context information for personalization purposes. Albeit employing different theoretical models like uses and gratification theory (e.g., Chiu and Huang 2014; Sutanto et al. 2014), social capital theory (e.g., Dinev et al. 2006, MaksI and Young 2013), or

the theory of planned behavior (e.g., Shibchurn and Yan 2015; Wirth et al. 2019), they all have in common that they predominantly view self-disclosure decisions as an outcome of perceived service benefits and costs, which are usually defined as privacy risks or sometimes concerns (Li 2012). In this regard, costs are subtracted from benefits and if the outcome (i.e., net value) is positive, self-disclosure is probable (e.g., Awad and Krishnan 2006):

$$\text{Benefits} - \text{Costs} = \text{Net Value}$$

This rationale is rooted in the social exchange theory (Homans 1958) and has formed the basis for the privacy calculus theory (Culnan and Armstrong 1999; Dinev and Hart 2006) which manifests the underlying theme of this thesis. The privacy calculus argues that benefits (privacy risks) positively (negatively) influence self-disclosure intentions/behavior (e.g., Krasnova et al. 2010a; Xu et al. 2009). It builds on the assumption that individuals engage in effortful and extensive information processing before making a decision (Dinev et al. 2015; Laufer and Wolfe 1977). Hence, building on the privacy calculus, research assumes that Internet users act based on a deliberate analysis taking into account their benefits and privacy risks (Li 2012).

Beyond the Privacy Calculus

Even though the privacy calculus is a plausible theory demonstrated in many studies, it might not capture the full complexity and nuances of self-disclosure decision-making against the background of other dynamics (Dinev et al. 2015). For instance, when it comes to actual self-disclosure users seem to act in opposition to their stated privacy concerns (e.g., Norberg et al. 2007) such as on SNS or other privacy-invasive information systems. The gap between stated privacy concerns and actual disclosure behavior is termed privacy paradox (e.g., Adjerid et al. 2018; Norberg et al. 2007) and has recently received much research attention (Adjerid et al. 2018; Kehr et al. 2015; Li et al. 2017). Beyond paradoxical disclosure decisions, research building on the privacy calculus perspective is not consistent across contexts. While some IS studies found empirical evidence for the privacy calculus (Krasnova et al. 2010a; Shibchurn and Yan 2015; Xu et al. 2009; Zhao et al. 2012), other studies are contradictory (e.g., Brakemeier et al. 2016a; Cho et al. 2010; Kehr et al. 2015). All in all, this indicates that there must be interference factors which distort individuals' situation-independent privacy judgements (see Figure 1). For instance, if a firm is successful in mitigating users' privacy risks by trust building mechanisms or other privacy indicators, while providing a great amount of benefits, users might be more willing to disclose their data to them (e.g., Chelappa and Sin 2005; Xu et al. 2005).

Building on behavioral economics, research identified two potential challenges which are devoted to privacy-related judgements, namely lack of information and motivation (Angst and Agarwal 2009; Dinev et al. 2015; Lowry et al. 2012). First, people lack complete information to make stable privacy decisions across contexts and against the background of their preferences (Kokolakis 2017). Whereas benefits are easy to anticipate (Acquisti 2004), perceived privacy risks are hard to evaluate (Smith et al. 2011). Individuals are mostly unsure of how, when, and to what extent their data will be used (Acquisti and Grossklags 2005b, 2005a). They might have disclosed it to one provider for making an online transaction, but the very same information can be also used to personalize products, target advertisement or business analytics. In this vein, they have to rely on their own knowledge, experiences, external information like privacy seals (Xu et al. 2005) or legislative rules (Metzger 2007). However, even when all information are available, cognitive psychology research argues that it is almost impossible to process all of them (Kahneman et al. 1982). Against this background, individuals apply certain simplifications which are referred to as

heuristics that help them to cope with their processing limitations (Barnes 1984; Kahneman et al. 1982). Even though heuristics help in overcoming the complexity of privacy decision-making, it eventually leads to decisions which are not in line with ones' preferences (Kokolakis 2017) as they may not have considered important information. Beyond the challenges of having all necessary information at hand to make well-informed privacy decisions, people need to be motivated to invest time and resources in evaluating privacy risks. For instance, Internet users might lack motivation to read long and complicated privacy policies. Indeed, in a recent poll only about 20 percent state that they read privacy policies completely (Auxier et al. 2019). This may cause a lower disposition to users' privacy risks and thus yield unstable disclosure decisions across contexts (see Figure 1).

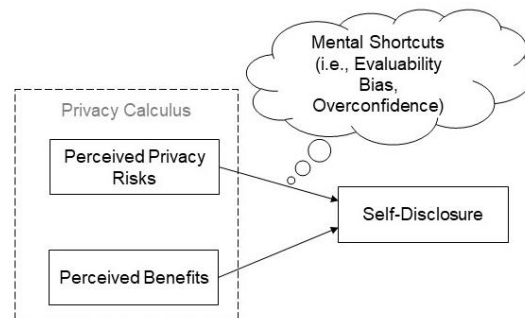


Figure 1. Biases in privacy-related judgements.

In this vein, scholars recently started to question the sole focus on benefits and risks (Dinev et al. 2015; Kehr et al. 2015; Lowry et al. 2012) taking into account situational factors which affect self-disclosure or even induce irrational choices. For instance, scholars have shown that stereotypical thinking (Gerlach et al. 2019), optimism bias (Baek et al. 2014), as well as affect heuristic (Kehr et al. 2015) can distort rational privacy-related judgements. Table 4 illustrates mental shortcuts which are tested in privacy research to help explain why privacy risks are not always linearly related to Internet users' willingness to self-disclose.

Table 4. Articles on mental shortcuts in privacy-related judgements.

Mental shortcuts	Articles
Regulatory Focus	Brakemeier et al. (2016); Mostelleri and Poddar (2017)
Endowment Effect	Acquisti et al. (2009)
Immediate Gratification	Acquisti (2004)
Stereotypical Thinking	Gerlach et al. (2019)
Optimism Bias	Baek et al. (2014); Cho et al. (2010)
Bounded Rationality	Acquisti and Grossklags (2005a); Keith et al. (2012)
Reference Dependence	Adjerid et al. (2018)
Cognitive Appraisal	Li et al. (2017)
Psychology of Ownership	Spiekermann et al. (2012)
Affect Heuristic	Kehr et al. (2015)
Information Asymmetry	Egelman et al. (2009); Tsai et al. (2011)

Beyond mental shortcuts, Internet users' privacy-related decision making might be prone to the context in which they are made. In this regard, research has shown that especially in the SNS context, the privacy calculus needs to be revisited (Wirth et al. 2019, Krasnova et al. 2009a).

Calculus for Social Networking Sites

Stemming from e-commerce literature, the privacy calculus focuses on users' concerns of releasing personal information such as name, bank details, or address to a provider as the only potential disadvantage arising from self-disclosure (Dinev and Hart 2006). However, communicating to other users online in order to establish relationships and thus intimacy differs (Choi and Bazarova 2020). In the SNS arena, through self-disclosures users voluntarily reveal identity cues. By sharing updates about their accomplishments and feelings, they are trying to establish a social image which is perceived, evaluated and critically assessed by a large and diverse audience on SNS (Barasch and Berger 2014).

Instead of solely focusing on organizational privacy threats, the fear of being misperceived or even rejected by peers expands the privacy calculus by adding social concerns to the privacy risk-benefit analysis. Social concerns are dealing with individuals' worries of how they are viewed in the eyes of others. It is the potential loss of one's self-image when being perceived as foolish or untrendy (Featherman and Pavlou 2003; Lee et al. 2013). More specifically, the social perspective acknowledges how impressions are formed and how they shape the desired social image (Goffman 1975; Leary and Kowalski 1990).

While online self-disclosure has been consistently linked to positive outcomes for senders, including improved self-esteem (Gonzales and Hancock 2011) or subjective happiness (Kim and Lee 2011), there has been growing evidence about the negative consequences of this activity for recipients. For example, studies have linked consumption of information shared on SNS to feelings of envy (James et al. 2017; Krasnova et al. 2015), depression (Tandoc et al. 2015), and reduction in one's life satisfaction (Frison and Eggermont 2016; Krasnova et al. 2015). Indeed, while senders indulge in sharing positive sides of their lives, recipients are getting the feeling that others have a better life compared to themselves, which leads to upward social comparison as well as perceptions of inferiority and low self-esteem (Fox and Moreland 2015; Frison and Eggermont 2016; Krasnova et al. 2015; Vogel et al. 2014). In light of these negative outcomes for recipients, there is a pressing need to better understand the dynamics behind self-disclosure in general and self-presentation on SNS in particular.

Compared to face-to-face (FtF) communication, the reactions of the audience towards the disclosed message are not visible and are asynchronous in nature (Walther 2007). Therefore, SNS users have to anticipate whether their self-disclosure socially pays off and whether it does contribute to relational benefits (Berman et al. 2015; Scopelliti et al. 2015). However, due to asynchronous feedback cycles and diverse or even ill-defined audiences, SNS users face a challenge when anticipating others' perception or reactions (Barasch and Berger 2014). In this regard, SNS users seem to selectively self-present when sharing their emotional experiences (Qiu et al. 2012), experiential accomplishments (Lyu 2016), positive emotions and well-being (Lin et al. 2012) compared to FtF communication. According to Lee et al. (2016), this propensity to consciously select photos that present oneself in the best light is fueled by 'likes' users get from their audiences. Additionally, self-disclosure in the sense of self-presenting oneself in front of others is encouraged by multiple functional affordances – IT artifacts – that, among others, include photo-editing features with the help of convenient filters or ability to easily communicate to a wide audience of followers (see Table 5).

Table 5. SNS artifacts.

Artifacts	Definition	Reasoning
Opportunity to invest effort into message construction	Users' tendency to invest time and effort in planning and creating the message to be shared.	Asynchronous communication gives SNS users the chance to consciously think about their message before sharing it (Walther 1996).
Message editability	Extent to which users rely on tools to edit their messages according to their impression management goals.	SNS photo-editing tools make it easy for users to edit the information being shared (Fox and Rooney 2015; Lyu 2016; Walther 2007).
Expectancy of positive feedback	Degree to which positive feedback is expected.	On SNS, positive feedback is intensified by the lack of other (negative) social cues (Walther 1996).
Immediate feedback	Degree to which feedback from the audience comes in in a quick and accessible way.	Compared to FtF communication, feedback on SNS comes fast and in an easy accessible form, because receivers may react by using the 'like' button or similar icons.
Social awareness	Degree to which the sender is aware of its audience and understands it.	On SNS, users are mentally and physically isolated from their audience which reduces social cues and social presence of the audience (Barasch and Berger 2014; Goel et al. 2011; Lowry et al. 2016).
Audience size (publicity of self-presentation)	The size of the audience who receives the information.	SNS facilitate communication to a large audience (Utz et al. 2012). Thus, SNS users in most cases communicate publicly to a greater audience compared to FtF communication.
Audience diversity	Degree to which the audience is heterogeneous.	On SNS, users are usually communicating to a heterogeneous audience which compromises close friends, distant acquaintances, colleagues and even strangers (Bernstein et al. 2013).

To sum up, this thesis adds to online self-disclosure literature in general and privacy calculus theory in particular by accounting for additional factors that could influence online self-disclosure decisions beyond benefits and privacy risks. To accomplish this goal, eight studies across different contexts (e.g., data-selling platforms, mobile applications) and decision stages (i.e., measuring valuation of privacy, intention to disclose personal information, and perceptual differences of shared information) have been conducted which are presented in the following.

3 Research Paper 1.A: Value of Privacy

Title: Putting a Price Tag on Personal Information - A Literature Review
Authors: Wagner, Amina; Wessels, Nora; Buxmann, Peter; Krasnova, Hanna
Published in: Hawaii International Conference on System Sciences (HICSS), Waikoloa Village, Hawaii, 2018

Abstract

In the digital age, personal information is claimed to be the new commodity with a rising market demand and profitability for businesses. Simultaneously, people are becoming aware of the value of their personal information while being concerned about their privacy. This increases the demand of direct compensation or protection. In response to the commodification of privacy and the increased demand for compensation, a number of scholars have shed light on the value people assign to their personal information. However, these findings remain controversial as their results differ tremendously due to different research methods and contexts. To address this gap, we conducted a systematic literature review to gain insights into the current research state and to identify further research avenues. By synthesizing and analyzing 37 publications, we provide an integrative framework along with seven contextual factors affecting individuals' valuation of privacy.

Keywords: Economics of Privacy, Literature Review, Personal Information, Privacy Valuation, Willingness-to-Pay

Introduction

The valuation of personal information is more relevant today than ever before because personal information is claimed to be the new commodity of the 21st century with a rising market demand and profitability for businesses (Spiekermann et al. 2015a). Particularly, online businesses like Facebook, Google & Co. monetize their users' personal information. Simultaneously, people are becoming aware of the value of their personal information (Li et al. 2014) which increases the demand of direct compensation and participation (New York Times 2012; Spiekermann and Korunovska 2017). In response to the trend of monetizing personal information, startups (e.g., datacoup, datafairplay) have emerged developing an infrastructure for users to actively sell their personal information to third parties. Indeed, increasing scholarly attention has been brought to the economics of information reflected by the growing number of studies in this field. More specifically, research has been conducted on how much people are willing to pay in order to protect their personal information and how much they demand for selling their data. However, sometimes it appeared as if people were incredibly privacy concerned and hence highly valued their data (Barak et al. 2013; Huberman et al. 2005) while other studies indicated that people do not value it at all (Bauer et al. 2012; Grossklags and Acquisti 2007). Even when researchers asked for the same type of data to be revealed, they obtained two completely different results. For instance, Huberman et al. (2005) showed that participants would sell their weight information for \$74.06 on average, whereas the study of Grossklags and Acquisti (2007) resulted in a price of \$31.80 for the same kind of information. Furthermore, Schreiner and Hess (2015) showed that Facebook users would pay on average 0.63 euro for a premium version while the study of Krasnova et al. (2009b) resulted in a monthly fee of 1.2 and 1.4 euro for a privacy-enhanced social networking site (SNS).

As these results are confounding and scattered, it is important to understand the differences between scholars to get insights into the valuation of privacy and how it is affected. Moreover, a systematic approach to comprehensively describe the current research state is missing despite its importance to provide an integrative and common understanding of individuals' valuation of privacy. Furthermore, businesses can only partially rely on knowledge when offering services which affect privacy concerns of their customers. To address this practical and theoretical issue, we conducted a structured literature review to provide a narrative theoretical survey, comparison, and integration of current literature. Thereby, the following research question will be answered: *What influences the economic value people assign to their personal information and how can the existing approaches and results be conceptualized in a unified way?*

Building upon established structured literature review methods (von Brocke et al. 2009; Webster and Watson 2002), we analyzed empirical studies within 37 publications published in various journals, conferences, and workshops. We coded the determinants of privacy valuation along with its research methods. These were then summarized in a twofold pattern including an in-depth look at underlying differences seeking to synthesize the resulting knowledge into an integrative theoretical framework (Baumeister and Leary 1997). Along with the determinants, willingness-to-pay and willingness-to-accept are then introduced as the two facets of how valuation of information is measured. Afterwards, we summarize and synthesize our main findings in an integrative theoretical framework. Findings are discussed and future Information Systems (IS) research suggestions are given before the paper closes with a conclusion.

Valuation of Privacy

Since privacy is monetized by firms (Steinfeld 2015), it can be exchanged by individuals in order to gain certain benefits. Referred to as the privacy calculus, people are performing a trade-off between privacy risks and benefits when assessing the behavioral intention to disclose information (Dinev and Hart 2006). Based on Smith et al. (1996) risks can be categorized into four dimensions: collection, improper access, error restrictions and secondary data usage. With regard to benefits, they should be perceived as higher than risks when revealing personal information (Rust et al. 2002; Xu et al. 2011a). Scholars found proof that people exchange their personal information to gain advanced services (Chelappa and Sin 2005) or monetary rewards (Hann and Lee 2002). Thus, understanding the value people put on their personal information is necessary for businesses to provide services accordingly. But personal information is different from other traded goods as the value people assign to their privacy is difficult to assess and generally subjective (Grossklags and Acquisti 2007). Further, people do not have valid and complete information of how their personal information will be used by businesses (Acquisti et al. 2009).

In an attempt to operationalize the valuation of privacy, previous scholars relied on surveys (e.g., Rose 2005) and experiments (e.g., Steinfeld 2015) measuring the amount of data which is revealed and shared with third parties as a form of privacy valuation (Hann et al. 2007; Krasnova et al. 2009b; Tsai et al. 2011). More specifically, they investigated what determines individual's privacy valuation and how privacy is traded by either measuring their willingness-to-pay (WTP) or their willingness-to-accept (WTA).

WTP for privacy deals with the fact that individuals prefer to pay a fee for privacy-enhancing features. It is referred to privacy premium which is typically offered by companies as a freemium product. Following the freemium idea, businesses provide their basic products free of charge while offering fee-based additional services (Schreiner and Hess 2015). In contrast, WTA describes individuals' willingness-to-sell data in return for monetary benefits (Acquisti et al. 2009). Thus, WTA describes the proposition that individuals respond to economic incentives in deciding whether to reveal personal data to a third party (Grossklags and Acquisti 2007) by taking an active role as a seller.

Review Method

In the following section, we provide an overview of our review method to identify the relevant literature by following the guidelines by von Brocke et al. (2009) and Webster and Watson (2002). By doing so, we describe the search term as well as the inclusion and exclusion criteria and present an overview of the conducted search process with its data sources. We describe the steps in detail in order to make the underlying process as transparent as possible following a call for more rigor (von Brocke et al. 2009).

With regard to our search terms, we conducted a pilot search based on the keywords used in prominent articles on privacy valuation (Carrascal et al. 2013; Hann et al. 2007; Huberman et al. 2005; Krasnova et al. 2009b; Tsai et al. 2011) as a starting point and refined this commencing search string iteratively. As the search query is crucial, the terms were selected precisely so that they sufficiently match the topic under investigation (von Brocke et al. 2009). Given the variety of keywords describing the "valuation of personal information" we divided this rudimentary term in its main components and searched for synonyms and related expressions. Finally, the final search string consisted of four parts. The first part comprises synonyms for "value" as this is the main

approach of our study. We used a number of search terms ranging from “economics”, “value/valuation”, and “worth” to terms describing pricing approaches. Of course, we also included “willingness” as it is the main component for WTA and WTP. The second part consists of different expressions for “personal” while the third part included the synonyms “information” and “data”. The last part of the final search query delimits the topic under investigation as the pilot search revealed that the topic received scholarly intention with the rise of ecommerce and SNS. This resulted in the following search query: ((“economics” OR “worth” OR valu* OR willingness-to* OR “freemium” OR “pricing”) AND (“privacy” OR “personal” OR “private”) AND (“data” OR “information”) AND (“online”)).

In order to ensure that only appropriate and relevant publications are included and that every paper incorporated in this review process is treated in the same way, we determined exclusion and inclusion criteria (Webster and Watson 2002). Inclusion criteria were defined as: (1) valuation of privacy and personal information was the main focus under investigation, (2) studies applied should be empirical and on an individual-level, and (3) studies investigated user’s monetary WTP and/or WTA in order to protect or divulge their personal data. In contrast, exclusion criteria included: (1) studies focused on privacy and personal data in general without examining the monetary value of the former, (2) the studies concentrated solely on testing measurement methods to evaluate privacy values or (3) were published before 2000 due to its validity in the online context.

In the next stage, we selected appropriate scientific databases which contained relevant publications (Webster and Watson 2002). The above presented search query was used for the EBSCOhost database whereas queries for other databases differed slightly due to its technical requirements. Finally, we conducted a systematic search in the following digital databases: ACM Digital Library, AIS Electronic Library, EBSCOhost Business Source Premier, ScienceDirect, SpringerLink, and WebOfScience. In order to be exhaustive, we decided to search by title and abstract without further restrictions with regard to specific journals, conferences, and topics. Second, we conducted a manual search in eight leading IS journals in the senior scholars’ basket of journals (i.e., Management Information Systems Quarterly, Information Systems Research, Journal of Management Information Systems) and in the IEEE publication list to ensure that no major IS or technology research articles were neglected. All found publications were uploaded into a Citavi database. Our search resulted in 1169 publications (excluding duplicates) for all selected databases in total. Next we scanned the titles and abstracts based on the selection criteria, which reduced the sample size to 114. By applying full text analysis, the sample was again minimized to 17. As suggested by Webster and Watson (2002) we also conducted a forward and backward search on this set of relevant publications. The process of backward search refers to the analyses of citations in the selected set of publications. In contrast, forward search aims at identifying publications that cite the selected key papers (Webster and Watson 2002), which was conducted by utilizing respective functions of Google Scholar. During forward and backward searches, we applied the same procedure as described before by identifying potentially relevant publications through their titles and abstracts and further investigating them with a full text analysis. Finally, we obtained a concluding set of 37 publications published between 2002 and 2017 which was the basis for further analyses and discussion.

Integrative Framework

After collecting the relevant literature, we coded the publications with regard to their research approaches and aggregated the results in a Table (see Appendix 3). Subsequently, we followed

suggestions by Baumeister and Leary (1997) and consolidated the results of our literature review in an integrative theoretical framework (see Figure 2) going beyond solely describing previous studies (Baumeister and Leary 1997; Webster and Watson 2002).

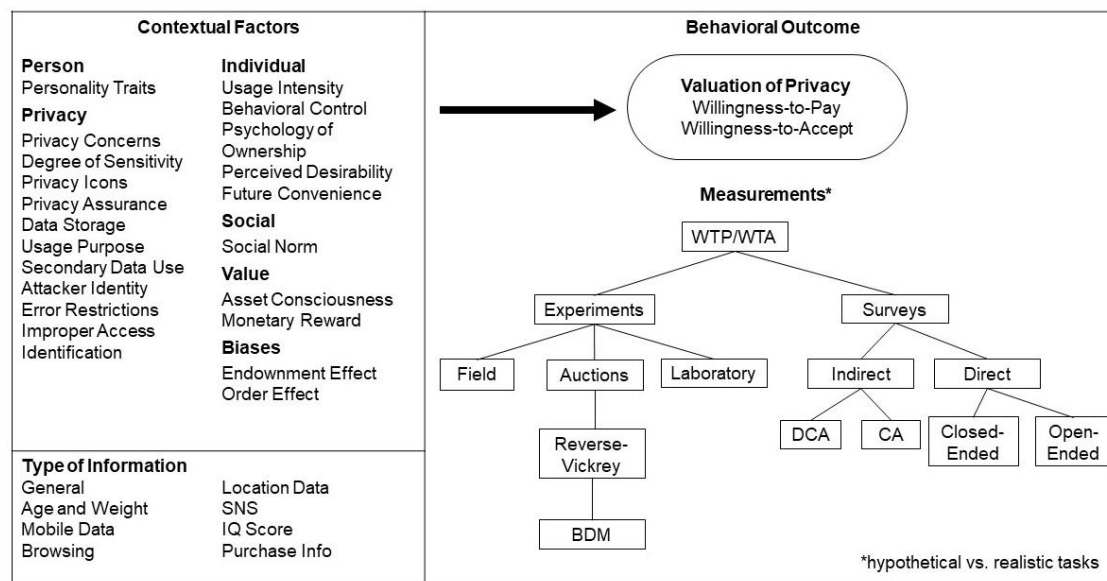


Figure 2. Integrative theoretical framework of valuation of privacy.

In accordance with previous privacy literature (Brandimarte and Acquisti 2012), we identified the context as highly relevant for users' privacy valuations. While synthesizing the literature, seven contextual factors emerged: type of information, person, biases, individual, privacy, value related, and social factors. These determinants affect the valuation of privacy. As all of the publications in our final sample implicitly divide context factors and behavioral outcome, a twofold pattern was chosen. A detailed summary of these patterns follows.

Contextual Factors

First, we identified the factor type of information which is determined by the research case of being highly relevant. All publications apart from Rose (2005) tested the impact of requests for certain types of information on individuals' privacy valuations. The type of information being evaluated by individuals ranges from SNS profile (10 papers), browsing information including websites (7 papers), purchase information (7 papers), location data (8 papers), mobile data (5 papers), IQ scores (2 papers), age and weight (2 paper) as well as general information/socio-demographics (4 papers). When authors investigated the value of SNS information, Facebook was used as the case distinguishing between all information stored on Facebook (Bauer et al. 2012; Spiekermann et al. 2012), the Facebook wall, or profile information (Benndorf and Normann 2014). Among others, studies also tested peoples' privacy valuations in the context of web browsing by for example investigating the WTP for a privacy friendly search engine (Bughin 2011). In addition, the valuation mode has been identified as a determinant of privacy valuation. A few studies built on behavioral economics and tested certain biases which affect the value individuals assign to their data (Kamleitner and Haddadi 2016, Acquisti et al. 2009, Grossklags and Acquisti 2007). Providing evidence for the endowment effect with regard to privacy valuations, Acquisti et al. (2009) demonstrated that participants valued their personal information even more when being asked to give it up compared to receiving it. This bias has also been confirmed by Kamleitner and Haddadi (2016) in the context of privacy as a possession.

Moving beyond the type of information which is often determined by the research case and behavioral biases, other contextual factors have been identified as having a direct impact on individuals' WTP/WTa. The dispositional factor person comprises personality traits. Staiano et al. (2014) investigated the influence of personality traits on peoples' WTa. They found no significant correlations between bid values and personality traits apart from agreeableness. Further, some scholars controlled for demographics. For instance, Cvrcek et al. (2006) showed that median bids of women are higher compared to men but interestingly the vast amount of studies found no significant differences for age, gender, and income (Carrascal et al. 2013; Egelman et al. 2012; Steinfeld 2015).

Furthermore, as the awareness of risks while sharing information online increases, we identified the factor privacy as another contextual determinant. According to Grossklags and Acquisti (2007), privacy preferences are the major antecedent for WTP and WTa. Looking at general privacy concerns, a great body of literature showed that valuation of privacy is negatively affected by the dispositional determinant 'general privacy concern' (Brush et al. 2010; Preibusch 2015; Staiano et al. 2014; Tsai et al. 2011). This is also exemplified in the study undertaken by Steinfeld (2015) demonstrating that abstainers are predominantly rejecting the offer due to higher privacy concerns compared to the group of traders. Egelman (2012) classified the participants according to Westin's metric into Privacy Fundamentalists, Privacy Unconcerned, and Privacy Pragmatists (Westin 1991), but found no significant differences. In contrast, Nguyen et al. (2016) used the same metric and observed major differences between those groups.

Apart from general privacy concerns, scholars investigated different privacy antecedents by manipulating or framing perceived privacy issues. Hann and Lee (2002) explored the effect of three subcategories of privacy concerns (errors, secondary use, and improper access) building on the privacy definition of Smith et al. (1996). Secondary data use was found to be the major driver of valuation of privacy which is also acknowledged by Potoglou et al. (2013) and Preibusch (2013). Beyond that, identification (Barak et al. 2013; Carrascal et al. 2013; Preibusch 2015; Regner and Riegner 2017) caused an increased demand for compensation whereas obfuscation decreased it (Brush et al. 2010). In addition, Egelman et al. (2009) provide evidence that when buying a privacy-sensitive good, people are more reluctant to pay for privacy. Similarly, Danezis et al. (2005) stated considerable differences between the WTa for academic and commercial use. When the participants were told that their data will be used for commercial purposes their bids roughly doubled. In sum, many privacy related antecedents were tested in literature.

Although privacy related antecedents received a lot of attention in research, other factors like value have been identified as a major influence factor on privacy valuation. Spiekermann et al. (2012) demonstrated that asset consciousness drives the value assigned to SNS information whereas Steinfeld (2015) mentioned that the monetary reward offered in exchange for data is a major antecedent to explain peoples' disposition to trade their data.

Moreover, we identified individual factors such as the usage intensity or perceived desirability as antecedents determining one's perceptions and beliefs about a certain dataset. In the case of age and weight information, Huberman et al. (2005) found proof that information that is perceived as 'abnormal' is assessed as being more valuable than e.g., normal weight. Other scholars found proof that people are willing to trade their data to get future convenience in return (Hann et al. 2007; Hann and Lee 2002). Lastly, we classified social factors as Racherla et al. (2011) showed that social norms influence the willingness-to-pay for privacy.

Behavioral Outcome

Following the classification suggested by Grossklags and Acquisti (2007), we categorized the publications on valuation of privacy in WTP for privacy and WTA privacy invasion. With a share of 57% (21 papers), the majority of authors investigated WTP. According to the results of the literature review, one can assume that people do not value their personal information at all. On the social network front, people displayed a generally low WTP when being asked to simply save their Facebook profiles from deletion (Spiekermann et al. 2012). While psychology of ownership, meaning to see the profile as one's own property, was shown to be a driving factor for WTP; up to 62% were not willing to pay even a trivial amount to save their profiles from deletion. The result changes though when people are made aware that a third party is interested in their data and hence, were under the effect of asset consciousness. The share of people with a WTP of 0 euro drops to 40% and the average WTP increases by a factor of 3.4.

Additionally, Schreiner and Hess (2015) demonstrated that Facebook users would pay on average 0.63 euro while Krasnova et al. (2009b) found a WTP between 1.2 and 1.4 euro a month for a privacy-enhanced SNS. These slightly different amounts might be explained due to opposing privacy definitions. Schreiner and Hess (2015) described the Facebook alternative as being less intrusive with regard to advertisement. Krasnova et al. (2009b) goes beyond that and crafted a Facebook alternative which provides a higher level of customizability and privacy control.

When looking at privacy protection in the context of smartphones it also became apparent that people are rather averse using a smartphone application that has access to their SNS data (Krasnova et al. 2014). In order to avoid a feature such as the FB login people report to be willing to pay between 1.79 and 6.24 euro depending on the number of permissions the FB login option asked for. Further, people are willing to sell their data when a certain price range is reached (Barak et al. 2013; Carrascal et al. 2013). But the WTA differentiates when information is being used for academic purposes compared to commercial purposes (Danezis et al. 2005). When it comes to very sensitive information like age and weight, people seem to value the information the most, especially when the weight deviates from the standard (Huberman et al. 2005). An additional result was that people seem to be quite unwilling to sell their location data recorded by their smartphones with WTA values ranging from about 3 euro for a single time location share and between 22.5 and 43 euro for a whole month of observation (Barak et al. 2013). Those WTA amounts were among the highest observed throughout the review. It became clear that people are quite worried about such data that allows others to draw conclusions on their daily routines and places they visit. Further, high amounts were raised for weight information. Huberman et al. (2005) showed that participants would sell their weight information for \$74.06 while Grossklags and Acquisti (2007) resulted in a requested price of \$31.80 for the same kind of information. These conflicting amounts can be explained by the research design. Grossklags and Acquisti (2007) investigated the WTA by applying open-questions whereas Huberman et al. (2005) relied on a reverse-second-price-auction.

Contrary, search engine users seem to be rather reluctant when it comes to protecting their own browsing behavior data. The amount they were willing to pay monthly for a premium version of a search engine such as Google with enhanced privacy features seemed to be around 1.5 dollar. Furthermore, it was shown that information on web behavior in general, be it the shops or the websites visited, is valued less than information that is not only linked to the web behavior of the user but also to his offline identity (such as name, address, or income). The median WTA for data out of the former category was found to be around 7 euro whereas the latter one was valued at 25 euro (Carrascal et al. 2013). This is also exemplified by the study of Preibusch (2013) where

people appreciate privacy-enhancing features in search engines when it is offered for free but only 15% would pay a minor premium for it. However when privacy icons are shown, the share of people choosing the shop with better privacy conditions is significantly higher than without (Tsai et al. 2011). They would even pay a premium fee for it (Egelman et al. 2009).

Regarding the valuation of privacy, we found that all studies are related to one's own privacy except of one study focusing on the difference between own profile information and others' profile information. This study demonstrated that friends' privacy is less valued implying that people are 'privacy egoists' (Pu and Grossklags 2015).

While certain rules of thumb may be derived from the studies e.g., location data is valued higher than SNS or browsing information, the methods used to elicit peoples' privacy valuations have to be considered.

Measurement Methods

In the following section, we will provide an overview of different methods used in current studies for measuring the monetary valuation of privacy, in the form of WTA and WTP. The categorization is based on the classification framework for WTP measurement methods by Breidert et al. (2006). As demonstrated by Benndorf and Normann (2014) the measurement method has a non-trivial impact on peoples' valuation of privacy. They used two techniques to elicit valuation of SNS information which resulted in two different results. The description of the methods follows.

We identified both, direct as well as indirect surveys as a frequently used method for measuring the monetary valuation of privacy. Especially direct surveys with online-questionnaires were often used either with simple open-ended questions, asking for a particular value as a threshold, or closed-ended questions, where a given value has to be assessed by the participants stating simple yes/no-answers (Grossklags and Acquisti 2007). A special form of these direct surveys is the contingent valuation method (CVM) that can be appropriately used for the valuation of goods or services which do not have an established market-price yet (Spiekermann et al. 2012). At the base of a fictitious scenario, the participants can either be asked to state a particular value (Spiekermann et al. 2012) or they are making a discrete choice (yes/no) for a given price (Rose 2005). As most direct surveys are hypothetical in nature, indirect surveys like conjoint analysis (CA) and discrete choice method (DCM) are applied to reduce this problem. Conjoint analysis builds on a service with several different features. Consumers can then build a preference ranking out of the different product versions (Pu and Grossklags 2015). Therefore, it is possible to measure the relative importance of these features (Krasnova et al. 2009b). For instance, Hann and Lee (2002) varied the perceived privacy concerns with regard to error, improper access, and secondary data use that people encounter when visiting a website. Similarly to CA, the DCM considers a product or service as a combination of different attributes (Breidert et al. 2006). Participants are asked to choose one out of two or more hypothetical alternatives in order to measure the independent influence of product's attributes as well as the valuation of the different attributes (Krasnova et al. 2014; Potoglou et al. 2013). One type of the DCM is the binary choice method, which was used by Nguyen et al. (2016).

In contrast to surveys, other reviewed studies conducted field or laboratory experiments with real life consequences by measuring the WTA or WTP as actual behavior either locally in a laboratory setting or unbounded of a special location (Acquisti et al. 2009; Beresford et al. 2012; Preibusch et al. 2013). One of the laboratory experiments was conducted as a take-it-or-leave-it (TIOLI) experiment (Benndorf and Normann 2014). All aforementioned methods have in common, that they can be conducted independently of time and number of participants, contrary to auctions

where several participants need to bid in parallel. In all eight papers conducting an auction, Vickrey auctions (VA) were applied in a reversed way (e.g., Egelman et al. 2009). It is conducted with sealed bids whereas the winner with the highest bid wins, only having to pay the price of the second highest bid (Breidert et al. 2006). This forces the participants to release their true valuations, because too high or too low bids are not going to be successful. A special type of VA, the Becker-DeGroot-Marshak Mechanism (BDM) (Becker et al. 1964) can also be applied to the WTA/WTP context by giving participants the opportunity to state the price they are willing to pay to purchase a particular good, for example a premium version of a SNS. If the stated price is lower than or equal to a randomly set price, the good can be bought at the random price (Schreiner and Hess 2015).

Besides these differences of the measurement methods, the conducted studies varied also in the design settings of the task the participants had to fulfill. We identified hypothetical settings (20 studies in our sample), where people realize that they can accomplish the task without real implications for them as they are e.g., asked to imagine a specific situation (Roeber et al. 2015) or had to choose between hypothetical alternatives (Nguyen et al. 2016). Hypothetical studies may mitigate peoples' affect as the participants have no 'costs' stating an inappropriate value (Krasnova et al. 2009b; Singleton and Harper 2001). Contrary, some studies provide real consequences for the participants, as they realistically sell their data (Benndorf and Normann 2014; Brush et al. 2010) or have to do a real purchase (Egelman et al. 2009; Tsai et al. 2011). But also in these cases, the participants were aware of the fact that they took part in an experiment.

Discussion

In the following, we will discuss our major findings obtained from the analysis of the reviewed studies and present our deriving future research suggestions. As the literature review reveals, numerous studies were seeking to quantify the monetary value people assign to their data over the last 15 years. The literature is centered on experimental designs ranging from online settings to laboratory and field experiments. However, the monetary value of privacy remains controversial. Especially as the terms personal information and privacy encompass so many different kinds of data that can be sold or protected. Judging from the results of our review, it appears that the value proposition to individuals' privacy is generally low. Further, the results of studies facing the participants with real consequences indicate that sometimes even a trivial discount is enough to sell personal information and that even tiny sums of money are seen as simply too much to protect it. Based on our analyses, one can see that scholars either focused on a specific subset of information or a situation-specific context like secondary data use or privacy assurances.

First of all, the majority of studies investigating peoples' privacy valuation focused on WTP. But more and more startups emerge, that allow users to actively sell their personal information. Despite this trend, the knowledge about generalizable WTA is limited due to the very specialized scopes of the preliminary studies. Therefore, a comprehensive perspective on all variable attributes affecting WTA might be a big progress. Beyond that, future research can look at the impact of re-sharing data that has been sold to an organization and is further shared by the latter with other parties.

For all 37 identified publications, we summarized determinants and assigned them to seven contextual factors with regard to WTA/WTP. The amount of identified contextual factors reveal the diversity of the previous studies. Overall, two predominant contextual factors emerged:

privacy related factors and the type of information. While we found 11 subcategories of privacy factors, general privacy concerns and the degree of sensitivity of the data to be revealed were most widely used for both types of behavioral outcomes. All of these studies share one common result: the more sensitive the data and the more identifiable people are, the higher has been the price people attach to their data as they perceive higher risks.

In addition, it was shown that in some cases the reported values for WTA and WTP may appear to be high but that this may only be due to the way the research was conducted. According to the review, studies with real consequences should be conducted to elicit users' privacy valuation. Being incentivized, people raise more realistic amounts in order to protect or sell their data (e.g., Grossklags and Acquisti 2007). Thereby, a 'hypothetical bias' should be omitted in future studies. Additionally, as described earlier, the results of studies using direct surveys differed tremendously from those using experiments like auctions. One of the reasons of these results might be social desirability or the talk-is-cheap problem. Hence, we conclude that hypothetical studies may lead to inflated WTA and WTP values and their hypothetical nature is probably one of the causes for the privacy paradox (e.g., Huberman et al. 2005). Therefore, validity of these studies is questioned.

A weakness of the analyzed studies are the opposing definitions of privacy as well as how and why information is collected which caused confounding privacy valuations. Still, the more transparent data practices were presented, the higher has been the awareness of risks and thus the impact on peoples' economic valuation of privacy. Thus, when privacy information is easy accessible and plausible, people seem to react very sensitive to it. These studies are important to understand users' assessment in a specific context, but it is difficult to transfer them to a broader context with respect to complicated data policies, complex exchange partners, and indirect outcomes. As a result, research is not sufficient and satisfying in explaining peoples' inability to be consistent in their privacy valuation.

Looking at the theoretical contribution of prior studies, they are merely based on privacy literature while some use the privacy calculus and its underlying trade-off between risks and benefits as the conceptual model (Krasnova et al. 2009b, Nguyen et al. 2016). Just a few studies build on theories such as information-processing theory (Hann and Lee 2002, Hann et al. 2007), multi-attribute utility theory (Nguyen et al. 2016), theory of property rights (Rose 2005), and theory of planned behavior (Schreiner and Hess 2015). Future research can adapt and extend theories from other disciplines focusing on the decision process and peoples' knowledge and awareness as well as their confidence in their own judgements. Some suggestions would be evaluability theory (Hsee and Zhang 2010) and elastic justification (Schweitzer and Hsee 2002) as well as general biases lend from behavioral economics. As IS research is interdisciplinary in nature, it should highlight how IT drives the valuation of privacy which is oftentimes due to the way privacy information is presented. Taken together, it would be important to clarify the mixed effects of some critical antecedents to derive to a broader conceptualization of privacy valuations. Finally, more research should be devoted to understand moderating effects of WTP and WTA.

Lastly, the sample size and sample characteristics differ tremendously among the selected studies. Thus, some kind of 'selection bias' can be recognized. Studies are mainly conducted with students as participants (Brandimarte and Acquisti 2012; Dinev and Hart 2006; Li et al. 2014). Students are generally characterized by a lower reluctance to participate in scholars because they tend to be more sensitive to rewards and are easily reachable for researchers. This results in a very young sample compared to e.g., the field study of Acquisti et al. (2009). In addition, across all studies concerning the valuation of information, people have different cultural backgrounds ranging from

a purely German sample (Bauer et al. 2012; Krasnova et al. 2009b; Schreiner and Hess 2015) to a European sample (Cvrcek et al. 2006) and a US sample (Egelman et al. 2009; Tsai et al. 2011). Furthermore, many studies used SNS as the case. One can argue that SNS users are privacy unconcerned as they reveal their data for free to use social networking services in return. Taken together, this implies that current research is not sufficiently representative for all internet users.

To sum up, our structured literature review has shown that people are very context-sensitive when evaluating their privacy. Especially, the measurement method and thus the study design can have a tremendous impact on the elicited monetary value of peoples' data. Privacy concerns as a dispositional factor and sensitivity of data seem to be a major driver of valuation of data. The more sensitive the data and the more transparent privacy issues are presented, the higher is the monetary value people attach to their data.

Conclusion

The goal of this structured literature review was to determine the value people assign to their personal information and to conceptualize the preliminary approaches and findings in a unified way. We showed that the monetary valuation of personal information can be measured as how much people are willing to pay in order to protect (WTP) as well as how much they are willing to accept in order to sell (WTA) their personal information. Hence, we reviewed 37 publications examining at least one of these two forms of privacy valuation and synthesized them in an overview Table (see Appendix 3) which served as the basis for further analysis. This paper makes several contributions to IS research and practice. Our paper is the first to provide a comprehensive review of the empirical studies on individuals' valuation of privacy. Thus, we introduce a comprehensive, integrative theoretical framework of privacy valuation along with their contextual factors like person, type of information, biases, privacy, individual, social, and value driven antecedents. This theoretical framework can serve as a basis to conceptualize the context-dependent valuation of information and its underlying phenomena, as well as guide future empirical research in this field. For online companies relying on customers' information, the framework shows that individuals disclose their information when benefits are offered in accordance. Additionally, online companies are made aware which key factors can drive the valuation of privacy critically like linkage to offline identity and perceived desirability. For individuals, this paper highlights multiple factors that drive the awareness and consciousness such as transparent secondary data use and identification to increase their valuation of privacy.

4 Research Paper 1.B: Willingness to Sell Personal Information

Title: To Sell or not to Sell – Antecedents of Individuals' Willingness-to-Sell Personal Information on Data-Selling Platforms

Authors: Wessels, Nora; Gerlach, Jin P.; Wagner, Amina

Published in: International Conference on Information Systems (ICIS), Munich, Germany, 2019

Abstract

Today, Internet users mostly take a passive role in the market for personal information, as they provide companies their data in return for free services but not money. To increase individuals' compensation, platforms have emerged, on which users can sell their personal information. These platforms provide a particular interesting context for research on the value of personal information. Existing studies on this topic have often relied on artificial settings and highly specialized research contexts, leading to context-specific results. Contrary, data-selling platforms can serve as a natural context to investigate users' willingness-to-sell (i.e., valuation of) personal information. We conducted a two-step study among 299 Internet users including a qualitative study and a choice-based conjoint analysis to investigate the antecedents of users' willingness-to-sell information on data-selling platforms and their relative importance. We contribute to research by offering a comprehensive list of antecedents and their importance in the highly-promising context of data-selling platforms.

Keywords: Willingness-to-Sell, Willingness-to-Accept, Economics of Privacy, Data-Selling Platforms, Personal Data Markets

Introduction

The common and often used comparisons of personal data with “the new oil of the Internet” and “the new currency of the digital world”, demonstrate the importance of personal data in the time of data-driven business models that use customers’ profiles for commercial purposes (Kuneva 2013; Spiekermann et al. 2015b). Individuals’ personal information is traded as an asset between companies, advertisers, and data brokers who can generate high revenues based on their users’ data as exemplified by Facebook, whose average revenue per user increased to almost 35 US-Dollar per American and Canadian user in 2018 (Facebook 2019; Spiekermann et al. 2015a). Beyond that, data broker also profit from the growing databases of enormous proportions, as the following statement of Acxiom illustrates: “We currently manage large datasets for leading marketing organizations around the world, executing more than 1 trillion global data transactions per week” (last10k 2018 p. 12). Further, not only data-driven businesses profit from “the new oil,” but also more traditional companies who analyze their users’ data — for instance for personalized offerings, decreased transaction costs, or risk analysis of their customers (Spiekermann et al. 2015a).

It is striking that users, as the “real owners” of their data, take a rather passive part in this business by releasing their data in return for allegedly free services such as social networking sites, search engines, and similar. So far, monetary compensation is not provided to users. As a result, many users feel unfairly treated (Culnan and Armstrong 1999; Culnan and Bies 2003). A recent study reveals that 78% of the British interviewees perceived that companies benefit the most from sharing their data, while only 8% see themselves as beneficiary (DMA 2018). Another study indicates that Internet users are becoming more aware of their data’s value and a share of them even actively strives to monetize their personal data (Accenture 2015). Against this background, some initiatives have started to rethink the business around user data with the goal to actually compensate users for giving away their personal data (Haberer and Schnurr 2018). As a result, in the last years, more and more platforms have emerged on which users can actively “sell” different types of personal data to interested companies or to the platform provider who then acts as an intermediary, e.g., Datacoup or the recently founded platforms Vetri and Wibson. On these data-selling platforms, users can create a personal account, enter the information they are willing to sell, and receive monetary compensation in exchange. These data-selling platforms are an interesting, alternative approach for the commercial data markets, and in particular, they are a very fruitful research context for investigating individuals’ monetary value of personal information and its antecedents. In recent years, the value of personal information has received a great deal of attention from researchers and practitioners alike, as the role of personal information as a commodity has significantly increased in importance (e.g., Acquisti et al. 2013; Pu and Grossklags 2015; Spiekermann et al. 2012). One central approach to study individuals’ monetary value of personal information is to examine their willingness-to-sell (WTS) this information, and, in particular, the antecedents that determine this WTS (e.g., Benndorf and Normann 2014; Hann et al. 2007; Schudy and Utikal 2017). While an individual’s WTS offers an indication with respect to the monetary value this individual would demand for selling his or her personal information (Acquisti et al. 2013; Grossklags and Acquisti 2007), the antecedents of WTS are of high theoretical value, as they represent the factors that lead to an increase or decrease in this WTS (e.g., Danezis et al. 2005; Jentzsch 2014). As data-selling platforms are purely designed for the sale of personal information, they could serve as a very natural research context to investigate users’ valuation of their personal information and its antecedents.

Furthermore, existing findings with respect to individuals' WTS and its antecedents cannot simply be transferred to the context of data-selling platforms. While prior research that has investigated the monetary value of users' personal information provides valuable insights (for an overview, see Wagner et al. 2018a), these studies have often relied on relatively artificial experimental settings and/or highly specialized research contexts (e.g., Huberman et al. 2005; Jentzsch 2014). As we will illustrate in more detail below, this has led to scattered, partly contradictory results, which are highly specific to the particular studies' contexts (e.g., financial portals, mobile sensing applications) and thus are difficult to transfer from one context to another (e.g., Christin et al. 2013; Hann et al. 2007). Specifically, these prior studies have usually derived antecedents of users' valuations of their personal data in a deductive manner (e.g., Hann et al. 2007; Huberman et al. 2005; Roeber et al. 2015) and it is unclear, whether these antecedents reflect those factors that are salient drivers of the value of personal information from the users' perspective. Against this background, Buckman et al. (2019) have called for research about the monetary values of personal data in realistic contexts with multiple influencing factors.

This leads us again to data-selling platforms who offer great potential for studying individuals' WTS (i.e., the value of) personal information and, from a theoretical standpoint, its antecedents. Nonetheless, we currently lack reliable insights as to what salient antecedents of individuals' WTS personal information on data-selling platforms are. Against this backdrop, we try to fill this gap by raising the following research question: *What are antecedents of individuals' willingness-to-sell personal information on data-selling platforms from a users' perspective?*

To answer this question, we conducted a first inductive study (N = 49) aimed at exploring the salient antecedents of individuals' WTS on data-selling platforms from the perspective of the users themselves. While this qualitative study was useful for identifying relevant antecedents, it was less well-suited to assess whether some antecedents might be more important than others, again from the users' perspective. However, the relative importance of these antecedents is important for researchers who seek to better understand the underlying mechanisms that determine individuals' WTS, as well as for practitioners who need to know what drives individuals' WTS. Therefore, we raise a second question that we will answer in a second step, based on a conjoint study among 250 Internet users. For a selected group of antecedents (we will provide details on why and how these antecedents were selected below), we ask the research question: *What are the relative weights that users ascribe to a selection of antecedents of their willingness-to-sell personal information on data-selling platforms?*

The theoretical implications that result from this two-step study are twofold: (1) We provide a comprehensive overview of antecedents of willingness-to-sell personal data on data-selling platforms from the users' perspective, highlighting the multitude of antecedents affecting the value of personal information. (2) We show the relative impact of selected antecedents and found the amount of compensation, type of data, and the origin of the platform being the most important ones. Further, we identify three knock-out criteria that seemed to be required by potential users of such platforms in the specified form: no transfer to third parties, the right to be forgotten, and one-time deals as duration of disclosure. Beyond these, our study also aids providers of data-selling platforms to carefully design their websites considering the needs of their potential users and eventually increase their success. This would allow users to have a more active role in the data trading process and profit from data as the new currency.

The paper is structured as follows. First, we present the theoretical background in terms of related work on willingness-to-sell personal information and further explain the concept of data-selling platforms. In the third section, we give an overview of our two-step approach, before step one and

two are described with their methods and results. Subsequently, we discuss our results, limitations, and future research opportunities.

Related Work

Due to the emergence of data-based services and the increased importance of personal information for businesses, the need to understand the value individuals place on their personal data and its antecedents has increased. In this vein, research in the field of economics of privacy has started to investigate individual's willingness-to-pay (WTP) for privacy as well as willingness-to-sell (WTS) personal data more than a decade ago (Hann et al. 2002; Rose 2005). While studies on WTP are concerned with how much money users are willing to pay for enhancing their privacy (e.g., Krasnova et al. 2009b; Spiekermann and Korunovska 2017), the WTS literature examines users' willingness of revealing personal information in exchange for a monetary reward or other benefits and its amount (e.g., Danezis et al. 2005; Hann et al. 2007; Schudy and Utikal 2017).

Looking across the previous literature, it is striking that the contexts in which prior research has been conducted are highly heterogeneous in nature. For instance, Acquisti et al. (2013) examined shopping mall visitors' willingness to reveal information about their purchases by letting them choose between gift cards with different monetary values. Further studies have been conducted in other, often rather artificial settings such as auctions in which participants could sell their weight and age information (Huberman et al. 2005) or IQ-test results (Jentzsch 2014). With regard to individuals' valuation of data on platforms, online social networks (Krasnova et al. 2009b; Pu and Grossklags 2016) and e-commerce websites (Egelman et al. 2009; Tsai et al. 2011) have so far been the main focus of research. Thus, for example, Roeber et al. (2015) conducted a conjoint analysis among participants who were asked to imagine sharing their personal data with different organizations (e.g., online shops, health insurances, social networking sites) to investigate the participants' WTS in these contexts. These examples illustrate how much the research contexts in previous studies differ, for instance with regard to the different types of information under investigation and many other factors such as the study design, ranging from auctions, laboratory and field experiments to open- or close-ended questions in surveys (e.g., Acquisti et al. 2013; Barak et al. 2013; Benndorf and Normann 2014; Brush et al. 2010).

The results obtained by the variety of highly heterogeneous studies in this area strongly suggest that it is not possible to simply transfer the findings from one context to another. While some of the studies, for instance, suggest that users request very high amounts of monetary reward (e.g., Brush et al. 2010; Huberman et al. 2005), others indeed find a surprisingly high willingness-to-sell data, even for small rewards of a few cents (e.g., Grossklags and Acquisti 2007; Roeber et al. 2015). Consider the following example which shows that the monetary valuation of personal data even varies significantly for the same type of data between studies due to variation in other contextual factors. An auction study conducted by Danezis et al. (2005) has found that users are willing to sell their location information from their mobile phones for academic purposes for about 10 GBP and about 20 GBP if the same information was used for commercial marketing purposes. Starkly contrasting these findings are the results obtained by Cvrcek et al. (2006) who, based on an intercultural study, found that participants demanded 28 GBP for selling the same type of information for academic purposes. Blurring these findings even further, Brush et al. (2010) integrated obfuscation methods for enhancing location privacy in the study and did not find any differences in users' valuations with regard to the two different purposes (academic vs. marketing). In this study, revealing GPS information to a corporate as well as to an academic institution was valued by participants to a similar amount, namely \$100 (about 77 GBP based on

exchange rate in April 2019). Overall, it seems hardly possible to transfer insights from one study's context to another making it necessary to investigate interesting contexts such as data-selling platforms in separate studies.

Further, as already mentioned, existing studies have already investigated many antecedents that have an influence on the valuation of privacy. For instance, in the context of online social networks, antecedents such as usage intensity (Bauer et al. 2012), degree of sensitivity and identification (Benndorf and Normann 2018), as well as privacy concerns (Krasnova et al. 2014) were investigated, while studies with a focus on purchases on e-commerce websites, have, for instance, additionally investigated the impact of privacy indicators (Egelman et al. 2009) and order effects as well as data storage (Preibusch et al. 2013). Many of these former studies have each selected a limited set of antecedents to include in their investigation (e.g., Barak et al. 2013; Hann et al. 2007; Jentzsch 2014). Moreover, most of them have relied on deductive approaches to choose the presumed antecedents of participants' WTS their personal information without verifying whether these were the ones with the most impact from the users' perspective. What is problematic about this approach is that we do not know if these antecedents under investigation really include all antecedents that matter from the users' perspective and which uncontrolled impact omitted ones might have had on the results.

As mentioned, data-selling platforms are designed as environments where individuals can naturally sell their data. Hence, they provide an interesting research context for willingness-to-sell studies that is free of any confounding contextual factors that could distort individuals' value they attach to their personal information. Data-selling platforms share the fundamental idea of allowing users to give away personal data in exchange for monetary benefits. As early as 1996, Laudon had already proposed such markets where individuals could transfer the rights to their personal data to companies or intermediaries in return for compensation in order to allow users to share more in the success of the data markets (Laudon 1996, 1997). Since then, concepts like this has been further discussed and developed in research (e.g., Aperjis and Huberman 2012; Haberer and Schnurr 2018; Matzutt et al. 2017) and more and more platforms come to the market. The most widely-known platform is Datacoup. This platform allows users to connect with existing accounts of social networking sites, banking accounts, or even activity trackers and sell associated data directly to the platform provider on a weekly base (Datacoup 2019). The amount of monetary compensation is displayed immediately, but the actual payment can only proceed after reaching a threshold of \$5. Other examples of data-selling platforms are Datawallet and Wibson which follow a similar approach, except that they rely on smart contracts and blockchain technology in order to grant interested parties access to the users' data, who receive a compensation in exchange (Datawallet 2019; Wibson 2019).

Two-Step Study Design

In order to answer our research questions, we followed a two-step approach. In the first step, we aimed at identifying the antecedents of individuals' WTS on data-selling platforms in a qualitative study. We used an inductive approach in order to explore those antecedents that really matter from the user-perspective as the existing literature had mostly relied on antecedents that were derived in a deductive manner and could thus, have neglected antecedents that really impact the valuation of personal information. These identified antecedents served as a basis for our second step, a choice-based conjoint (CBC) analysis, that intended to investigate the relative weights of selected antecedents, represented as attributes for the CBC (as will be explained in more detail below). Figure 3 provides an overview of these two steps.

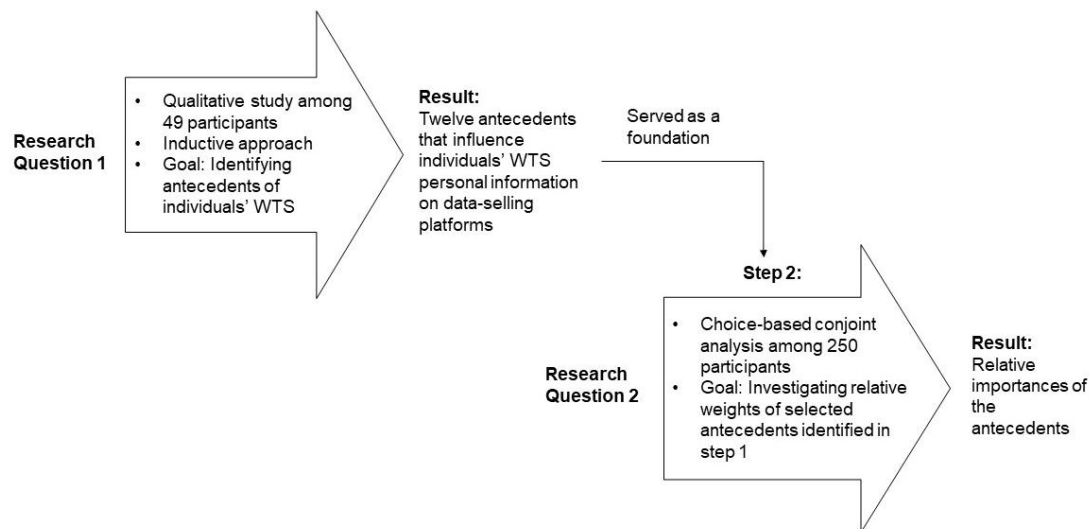


Figure 3. Overview of the two-step study.

Step One: Qualitative Study

Method

This first step was aimed at identifying a set of antecedents to an individual's willingness-to-sell personal data in an inductive manner. First, we defined the relevant target population against the background of our research question and agreed on a sampling strategy. As frequent Internet users are the most likely user group of personal data-selling platforms, we were interested in their thoughts and opinions. Therefore, we obtained a sample that matches the age and gender distribution for frequent Internet users (Statista 2014a; Statista 2014b). We developed an online survey including mockups of an online data-selling platform as well as open-ended questions. We relied on mockups for describing data-selling platforms as they provide participants with an adequate understanding of the functionality while simultaneously excluding variation due to differences between the existing platforms and to avoid biases due to branding/marketing by specific platforms. After an introductory page, the participants first had to read an explanation about these platforms and the data-selling procedure, and then three mockups were displayed. These mockups represented the most important pages of a data-selling-platform's website: The first page described the fundamental idea behind data-selling platforms that Internet users as the "real data owners" can sell the data they want to sell to partner companies of the platform and thus participate in the business around their personal information. The second mockup illustrated how a data profile might be created and exemplified data types that could be sold. The mockup also showed that individuals could decide on their own which data they want to reveal and that the amount of compensation for the selected set of data was displayed immediately. Finally, the third mockup displayed a users' account with the current balance and the possibility to prompt the payout. After the mockups were shown, our main question was displayed to the respondents: Under what circumstances would you be willing to sell your data on such a platform? We asked the respondents to provide open-ended answers and to describe at least four factors but they had the opportunity to describe more factors if they were willing to do so. We pretested the survey including the mockups among nine Information Systems (IS) researchers. Based on their feedback, adjustments were made iteratively in order to ensure clarity and comprehensiveness.

With the assistance of a survey company, 63 individuals from our European country were invited to participate in our study. We included an attention check by incorporating an instructed

response item to identify inattentive participants (Meade and Craig 2012) and five respondents who failed this check were excluded from the sample. Of the remaining 58 participants, nine of them stated that they would never consider selling their data on such a platform and therefore did not provide any answers to our open-ended question. Removing these respondents, the final dataset consisted of responses from 49 participants. The final sample yielded 21 females and 28 males, whereas 35% were between 18 and 25 years old, 35% were between 26 and 35, 10% were between 36 and 45, 10% were between 46 and 55, and 10% were older than 56. With a share of 37%, the majority were professionals followed by 29% students, 14% unoccupied, 12% self-employed persons, and 8% others or not specified.

To analyze the data, we used coding techniques offered by inductive qualitative study methods (Ryan and Bernard 2003; Saldaña 2015). Starting with an initial coding, we attached conceptual labels to participants' answers and therefore categorized the factors which were described by the respondents. We took care to identify all mentioned antecedents directly influencing the willingness-to-sell personal data but excluded those factors that are only provider-specific and therefore meet the requirements for several kind of platforms (e.g., effort to type in the data or recommendation of friends about the usage) as these do not directly influence the WTS. Subsequently, we merged some codes of this initial coding which were similar in meaning and subsumed some of them under a broader conceptual label. Three researchers coded the factors independently and merged or adjusted the factors accordingly in different rounds.

Results: Antecedents of Willingness-to-Sell

In sum, 12 antecedents of users' WTS personal information on data-selling platforms emerged from the data. As a result of the coding process we grouped these antecedents into eight broader categories. Table 6 presents an overview of the antecedents, their associated categories, and descriptions.

Table 6. Antecedents of users' WTS personal information on data-selling platforms.

Category	Antecedent	Description
Compensation	Form of Compensation	The form of the compensation for revealing the data (monetary reward or other benefits e.g., coupons, bonus, time savings)
	Amount of Compensation	The amount of money/benefit that is paid for revealing the data
Buying Instance	Buying Instance, e.g., Companies	Who is buying and using the data?
Data	Type of Data	Type of data and its sensitivity
	Anonymity	Do the data have a link to my identity? Or are they anonymous?
Purpose of Use	Purpose of Use	For what purpose will the data be used?
No Transfer to Third Parties	No Transfer to Third Parties	The buying instance should not be allowed to resell the data or at least must ask the data-selling person for permission.
Provider of the Platform	Trustworthiness	Is the platform provider a trustworthy company? Is the provider monitored from an independent instance? Is the platform provider reliable and serious? And what is its reputation?
	Origin and Legal Framework	Where is the company based? And what is the legal context?
Duration of Disclosure	Duration of Disclosure	Is it a single deal or is the platform acquiring a long-term right to receive up-to-date information about you (standing order)?

Security and Privacy	Security	Are the data protected against unauthorized access by a secure infrastructure (e.g., encryption)?
	Right to be Forgotten	Is it possible to exit from the process? What would be the consequence then? Is it possible to delete the data?

The participants frequently stated the compensation as having an impact on their willingness-to-sell personal data. Although the participants were asked under what circumstances they would be willing to sell data on such a platform, some interviewees could also imagine different forms of compensations and not only money. So they suggested benefits like coupons, special offers, time savings, or even job offers as possible compensations. But in the majority of cases, the participants requested a monetary compensation: “as I have to reveal my data anyway, why not getting a financial return for it”. In addition to the participants that were concerned about the form of compensation, most of the surveyed Internet users also mentioned the amount of reward as an important factor. They stated that the compensation should be “appropriate”, “as high as possible”, or “not just a few cents”. Two participants even specified concrete amounts for revealing their data (i.e., €500 and €1000).

In addition, some participants indicated that they care about which instance is buying the data: “I want to know who is buying my data and I am not willing to give it just to anyone.” So, participants at least requested transparency regarding the instance involved: “I want to know the company in advance (e.g., insurance business).” A few participants explicitly expressed the wish of being able to control the selection of companies involved: “Can I influence which companies are going to buy my data or can I specifically exclude some of them?”

The data itself and their sensitivity also played a significant role for the surveyed Internet users and was stated frequently. Some participants said that they would not sell their telephone numbers and/or address data; others were reluctant to provide photos or videos. One participant stated: “It all depends on the type of data I reveal. For me there are some data that I can reveal easily, but there are also some data that I would not like to reveal.” This seemed to depend on the level of the data’s sensitivity; one Internet user stated: “sports are not sensitive, but [my] recent medication is.” For some, the sensitivity also depended on the variability of data. One person for example said that he is more willing to give away email-addresses or even bank accounts, as these can easily be changed. Similar to the buying instance, participants also requested control over the choice of data: “I want to decide on my own which data to reveal” and a few interviewees also stated that it would have an impact on their willingness-to-sell if the data had a link to their personal identity or if they could stay anonymous.

Beyond that, many participants stated that their willingness-to-sell personal information depends on the purpose for which the data will be used. Some said they would only do it for “useful purposes” or “good reasons”, others stated examples like donations and scientific studies. One interviewee explained: “I would not do it for things that can be negative for me, like credit assessment.” Another frequently mentioned purpose was advertisement. One Internet user made a positive association: “One of the reasons of collecting data is that advertisement should attract me. In this case, the advertisement would be customized to me.” Contrary, another participant was afraid of undesirable advertisement: “If I would not be called ten times per day with offers of insurances, smartphones, lottery, or whatever, I would rather reveal my data.” In one case, the participation was even seen as idealistic, like the following quote indicates: “I want to change something with my data and enhance the company.”

Participants also stated that their data should be used “only for internal purposes”. This condition is represented by the factor: No transfer to third parties. This seemed to be a critical factor that can be exemplified by the following quote: “The data buying company should bound to pre-empt drawbacks for the data-selling person, by not re-selling the data to externals, which could injure the data seller financially or socially.”

Additionally, the origin of the provider and therefore the applicable law was identified as having an impact on the willingness-to-sell personal data. So, one participant for example requested “The company should be based within the European Union.” And another one expressed the wish to know the legal framework: “Which legal framework is given? Which law applies if it is a foreign company?” This antecedent was related to the platform provider’s trustworthiness, which was also stated by the participants. One of them indicated: “Revealing personal information is a delicate matter and I need to trust the company.” In order to enhance the trustworthiness, one interviewee suggested the establishment of independently controlled certifications, and another surveyed Internet user proposed a governmental control of the provider with public accessible results. Further, the platforms provider’s reliability and its reputation can also foster trust: “Who is buying my data? Is the company trustworthy? Will my data be safe? The company should present itself as reliable or—even better—it should be possible to assess the company, in order to see if it is really trustworthy.”

Furthermore, the duration of the disclosure, more precisely if selling the data would be a one-time deal or if the platform is acquiring a long-term right to receive this personal information was mentioned: “The reward should be variable and adequate. It could be either a single reward for particular data, or a dynamic reward sold over a longer period. Similar to the dynamics of life assurances compensating inflation—if the data gain in importance over time and still remain relevant after years, the customer should benefit accordingly.” Also, some surveyed participants were concerned about the question if platform users would be obliged to keep their data up-to-date, or if they can profit from changes. This can be exemplified by the following statement of one of the participants: “If I should marry, move, or get a raise, I should not be committed to update my data, but I want to profit again by providing the changes voluntarily.”

Finally, security and privacy related issues present another important category. Frequently, concerns about an appropriate level of security in terms of encryption, storage, and server infrastructure, and in general, an adequate protection against criminal acts were expressed: “On such a website, the security is incredibly important as I, for example, do not want to be a victim of hackers.” Similarly, some interviewees were also concerned about the threat of data misuse. This can be exemplified by statements like: “I am afraid of a loss of identity”, “my data should not be misused,” or “It should not be used to do dubious things so that I have to feel insecure in everyday life.” In order to reduce these worries, a kind of assurance was suggested where the company is responsible to compensate “sufficiently” in case of incidents. Further, some survey participants rose the privacy-related question about the “right to be forgotten” and therefore, if it would be possible to unsubscribe from the service and what the consequences would be, while another Internet user just stated: “If I request it, the data have to be deleted.”

These identified antecedents of willingness-to-sell served as a base for further investigation in the second step, which is described in the next section.

Step Two: Choice-Based Conjoint (CBC) Analysis

Method

In the next step, we were interested in the relative weights that users assign to a selection of the antecedents identified in the qualitative step. To answer this research question, we conducted a choice-based conjoint (CBC) analysis. This method allowed us to investigate situations in which potential users have to choose among platform alternatives that vary with respect to their characteristics (Green et al. 2001) and to analyze users' preferences respectively (Roßnagel et al. 2014). As our qualitative study had revealed several antecedents of individuals' WTS that can be all seen as characteristics or features of data-selling platforms, conjoint analysis presents an appropriate method to assess these antecedents' relative importance.

The underlying assumption of the conjoint method is that participants perceive alternatives in a decision making process as a bundle of certain characteristics or features, so-called attributes, which can take the form of different values, the so called attribute levels (Green and Srinivasan 1978; Pu and Grossklags 2015). Thus, we can draw inferences from the conjoint approach about the composition of utilities of data-selling platforms by investigating the partial utilities of the attribute levels as well as the average importance of attributes from a user perspective (Johnson 1974; Krasnova et al. 2009b). To do so, the conjoint method is based on a decompositional approach, in which utilities (i.e., part-worths) are calculated for the individual attribute levels in a way that these are most consistent with the respondent's overall preferences, as revealed by their choices throughout the conjoint study (Green and Srinivasan 1978). The traditional conjoint method analyzes decisions about trade-offs among alternatives by letting the individuals rate presented alternatives simultaneously (Green et al. 2001; Pu and Grossklags 2016). This rating-approach, however, is cognitively challenging for the participants (Braun et al. 2016) and it does not reflect individuals' real behavior in decision processes (Orme 2009). Therefore, we conducted a choice-based conjoint (CBC) analysis, which is assumed to be more realistic, cognitively less challenging, and a slightly better performer (Karniouchina et al. 2009; Pu and Grossklags 2015). In CBCs, participants only see a few alternatives simultaneously that differ with respect to their particular characteristics and have to pick the most preferred alternative from this set (Green et al. 2001). By applying Hierarchical Bayes, it is possible to estimate part-worth utilities at the individual-level, which can in turn be used to compute relative importance of the attributes (Braun et al. 2016). CBC is a widely used type of conjoint analysis and has also been frequently used in IS research (e.g., Dauda and Lee 2015; Hu et al. 2012; Penttinen et al. 2019; Roßnagel et al. 2014).

Determination of Attributes and Attribute Levels

As mentioned, 12 antecedents identified in the qualitative step served as a basis for determining the CBC-attributes, as these antecedents can be seen as characteristics or features of data-selling platforms. Due to methodological requirements, we had to eliminate a subset of these antecedents and only compare the relative importance for a selection of antecedents: First, attributes in a conjoint study must not be dependent on each other (Louviere 1988; Orme 2002). Assessing our list of antecedents regarding this requirement, a dependency existed between the type of data and anonymity, as different types of data vary in their degree to which they can be used to identify an individual (Milne et al. 2017). Likewise, trustworthiness of a provider depends on both the company's origin and legal framework as well as on the security offered (e.g., Cheung and Lee 2006; Flavián and Guinalú 2006; Perusco and Michael 2007). Therefore, anonymity and trustworthiness were excluded from the conjoint attribute list as these arguably depend on the other mentioned antecedents (and not the other way around). We further removed one

antecedent that seemed to be a knock-out criterion for potential users of data-selling platforms: Within the qualitative study all mentions concerning the antecedent “no transfer to third parties” indicated that the Internet users uncompromisingly requested a forbid of a transfer from the buying company to another third party. So, we decide to exclude this factor from the conjoint analysis as recommended in literature (e.g., Hensher 1994) by stating that the participants should assume the buyer does not transfer any personal information to any third party.

To further validate the remaining list of attributes and to determine appropriate manifestations, we followed suggestions by conjoint analysis literature (Green and Krieger 1991; Krasnova et al. 2009b) and relied on an inductive approach conducting another 21 semi-structured interviews among Internet users. Thereby, we first introduced the idea of data-selling platforms with the help of the mockups shown in the prior study. Afterwards, the nine remaining attributes (form and amount of compensation, buying company, type of data, purpose of use, origin and legal framework, duration of disclosure, security, right to be forgotten) were presented and interviewees were asked to comment on them and state possible levels of these attributes, either positive or negative ones. Based on these interviews two additional antecedents of WTS were removed for the conjoint task, as they represented knock-out criteria for our interviewees as well. Almost all respondents required the right to be forgotten and a one-time deal as the duration of disclosure type. This indicated that little variation with respect to these factors can be expected (Hensher 1994) and thus, we decided to fix them in our upcoming CBC as well by stating that the participants should assume that the platform always offers the possibility to delete personal information and that selling data was always a one-time deal. Further, most interviewees were challenged by the task to state manifestations of buying companies or industries. This indicated that the participants of our conjoint study might have difficulties to assess this attribute and its associated levels, which can lead to distorted or non-interpretable results. Thus, we excluded the buying instance from the conjoint analysis as well. For all other attributes, participants offered helpful suggestions for potential attribute levels. Making sure that the levels were mutually exclusive and clearly worded (Orme 2002) this procedure resulted in two to three levels for each attribute. An overview of all attributes and attribute levels used in the conjoint study is provided in Table 7.

Table 7. Summary of attributes and attribute levels of the CBC study.

Attribute	Levels
Type of Data	Address (e.g., Name, Street, City)
	Demographics (e.g., Age, Sex, Income)
	Personal Interests (e.g., Leisure Time, Fashion, Food)
Purpose of Use	Research and Development
	Advertisement
	Anonymized Statistics
Origin and Legal Framework	Western European Country (e.g., Britain, France, Germany)
	European Union
	United States
Security	Password
	Password and Encryption
	Password, Encryption, and Certification of Third Party
Form of Compensation	Money

	Coupons for Online Shops (e.g., Amazon)
Amount of Compensation	5€
	10€
	20€

Conjoint Design and Study Realization

As a conjoint design, we relied on a traditional full-profile CBC with three alternatives of platforms (so called concepts) per choice task plus a “no choice”-option. The “no choice”-option is of particular importance in this context, as the qualitative study had already demonstrated that some individuals are generally unwilling to sell their data. Every participant had to make 17 decisions among different configurations (i.e., choice tasks), that were implemented in Sawtooth Software. The CBC was embedded in an online survey similar in structure to the qualitative step with the same mockups and descriptions except for the additional statements regarding the knock-out criteria stating that the participants should assume that the platform always offers the possibility to delete personal information, that it is always a one-time deal, and that there will be no further transfer to third parties by the buying companies. As the interviews revealed potential difficulties for the respondents in evaluating different types of buying companies, we eliminated this degree of freedom by stating that partner companies of the platform were buying the data. Finally, participants were presented the actual choice tasks and, for each choice set, had to pick the alternative they would use (or the no choice option).

We collaborated with the same survey company used in the first step to collect data in a Western European country. We aimed to reach age and gender distributions which were representative for frequent Internet users as reported by Statista (Statista 2014a; Statista 2014b). We screened out 73 respondents due to a failed attention check, again realized with an instructed response item (Meade and Craig 2012), leaving 250 participants who answered the whole questionnaire. Therefore, the final sample of our second study consisted of 250 participants in total, 133 males and 117 females. From these participants 26% were between 18 and 24 years old, 27% were between 25 and 34, 20% were between 35 and 44, 14% were between 45 and 54, and 13% were older than 55 years. Again, most of the respondents were professionals with a share of 51%, while 20% were students, 8% were self-employed persons, 18% stated “others” or “not specified”, and 3% were unoccupied.

Results: Choice-Based Conjoint Analysis

In order to analyze the choice-decisions of the participants, we applied the Hierarchical Bayes method for estimating average utilities, that mirror the attractiveness of the levels as well as the relative importance of the six attributes (Pu and Grossklags 2015). As such, we can gain insights about the weights the users assign to each attribute while deciding which of the shown platform-alternative (including the no-choice) they would pick if they had the opportunity to do so. The results are depicted in Table 8. We further followed the approach of Krasnova et al. (2009b) and used the part-worths to compute utility changes from one level to another within one attribute, which deepen our understanding of a level’s attractiveness. These results are summarized in the column “Utility Changes” in Table 9. Additionally, we conducted t-tests on the null hypothesis that the part-worths are equal (p-values are shown in Table 9).

Comparing the average importancia of the attributes, the amount of compensation presents by far the most influential attribute with a relative importance of 27.36%. This result implies that

Internet users are inclined to sell their data if the reward is big enough. It is not surprising, that the utilities increase with the amount of money offered by the platform. However, the utility change from 5€ to 10€ is much bigger than the increase from 10€ to 20€, both being significant as revealed by the t-tests. Calculating the utilities per Euro, the utility increases by $83.38/5 = 16.68$ units from 5€ to 10€ and only $51.08/10 = 5.11$ units from 10€ to 20€, indicating a decreasing marginal utility. These values can also be used in the following analysis to calculate the monetary value of the changes between attribute levels (Krasnova et al. 2009b; Pu and Grossklags 2015). As the compensation does not increase in a linear fashion, we calculated these monetary values of changes for both €-equivalents 16.68€ and 5.11€ expressing upper and lower bounds of monetary equivalents. These results are presented in Table 9.

With a relative importance of 21.88%, type of data constitutes the second most important attribute as revealed by our analysis. A comparison of the utilities indicates that the participants clearly distinguish between different types of data and prefer non-identifiable data: While address data is the most unpopular type with a utility change of 74.68 (compared to demographics), the difference between demographics and personal interests is significant as well, but the utility change is only 27.93. In terms of monetary value change this implies an increase of a range between 4.48€ (lower bound) to 14.61€ (upper bound).

The origin and legal framework of the company offering the data-selling platform also turned out to be important with a relative importance of 18.03%. The highest utilities are found for specific Western European Countries, followed by the EU in general, but these differences are not significant. In contrast, a change to the US results in a significant utility decrease of 83.08. Thus, a utility increase resulting from a change in monetary reward from 5€ to 10€ could be almost completely compensated by the utility decrease caused by a move from the EU to the US. It is important to note that these results might be biased due to our Western European sample. Future research should complement our findings based on samples from different cultures.

The purpose of use also received noticeable average importance of 13.58%. The average utilities indicate that the participants dislike marketing purposes such as advertisements the most, and would rather prefer to sell their data for research and development as well as for anonymized statistics, the latter being the most preferred option. However, the t-test could not find significant differences between research and anonymized statistics as purposes of data use. Regarding the monetary value can the change between advertisement and research be depicted as a range between 3.35€ and 11.27€.

With an average importance of 10.88%, the form of compensation is the fifth most important attribute. The utility change of 51.68 shows a clear preference towards a monetary reward compared to coupons with the same amount leading to a significant decrease.

The least important antecedent is presented by the security factor. The results indeed show higher utilities for a higher security level, however, utility changes of 20.92 from the very basic level of simple password protection to the next level of password protection and encryption indicate that the respondents do not have high expectations regarding the security settings of such platforms. The utility change to the next level with an additional certification of a third party resulted in an even smaller utility increase of just 11.71 but the levels are significantly different.

Overall, these results indicate that the most preferred data-selling platform would provide a monetary compensation as high as possible (in this case 20€) for the sale of personal interests used for anonymized statistics or research and development. Further, the platform provider

should be located in a (Western) European country and offer a high security level such as password (PW) protection, encryption, and a certification of a third party.

Table 8. Attributes, levels, part-worths, and average importancia.

Attributes	Levels	Average Utilities (Part-Worths)*	Standard Deviation	Average Importancia
Amount of Compensation	5€	-72.61	67.02	27.36%
	10€	10.77	20.65	
	20€	61.843	77.43	
Type of Data	Address	-59.10	66.42	21.88%
	Demographics	15.58	37.44	
	Personal Interests	43.51	49.27	
Origin and Legal Framework	Western European Country	29.70	36.63	18.03%
	European Union	26.69	28.96	
	United States	-56.39	60.23	
Purpose of Use	Advertisement	-38.89	40.99	13.58%
	Research and Development	18.71	26.89	
	Anonymized Statistics	20.18	30.90	
Form of Compensation	Money	25.84	33.06	10.88%
	Coupons for Online Shops	-25.84	33.06	
Security	Password	-17.85	26.59	8.27%
	Password and Encryption	3.07	16.74	
	Password, Encryption, and Certification	14.78	27.39	
* The average utilities are scaled with zero-centered differences.				

Table 9. Utility changes and monetary value of changes.

Attribute	Level Change	Utility Change	P-Value (T-Test on Equality)	Monetary Value of Change in €
Amount of Compensation	5€ -> 10€	83.38	0.0001	
	10€ -> 20€	51.08	0.0001	
Type of Data	Address -> Demographics	74.68	0.0001	4.48 - 14.61
	Demographics -> Personal Interests	27.93	0.0001	1.67 - 5.11
Origin and Legal Framework	Western European Country -> EU	-3.00	0.3098	-0.18 - -0.59
	EU -> US	-83.08	0.0001	-4.98 - -16.26
Purpose of Use	Advertisement -> Research	57.59	0.0001	3.35 - 11.27
	Research -> Anonymized Statistics	1.48	0.5691	0.09 - 0.29

Form of Compensation	Money -> Coupons	-51.68	0.0001	-3.10 - -10.11
Security	PW -> PW and Encryption	20.92	0.0001	1.25 - 4.09
	PW and Encryption -> PW, Encryption, and Certification	11.71	0.0001	0.70 - 2.29

Discussion

The aim of our research was to identify antecedents of individuals' willingness-to-sell data in the context of online data-selling platforms (RQ1). Additionally, we examined the relative weights of a selected set of antecedents (RQ2). Based on a two-step study, and using data obtained from a total of 299 participants, we were able to identify 12 antecedents. We further found varying importancia between a selected subset of factors and found that Internet users have clear preferences for some of the investigated levels. We will discuss the theoretical and managerial implications of our study as well as limitations and future research suggestions in the following.

Implications of the Study

Commencing with the theoretical implications, we see two major contributions of our study. First, our study contributes to literature investigating the valuation of personal data, which is a topic of particular interest in the time of data-driven business models where data are traded as a commodity. While previous studies investigating the value that individuals assign to their data have often focused on rather artificial experimental settings and specialized research contexts, our study investigates the antecedents of Internet users' willingness-to-sell personal data in the purest data-selling context: on platforms that are solely designed for this purpose. These platforms are a highly promising context to study individuals' willingness-to-sell data and its antecedents. But, as illustrated by the highly heterogeneous findings of prior research, it is hardly possible to simply transfer the findings from prior contexts to ours, even in the area of other platforms like online social networks.

While our study is in line with some findings of previous studies in different contexts, such as individuals' preference for non-identifiable data (e.g., Benndorf and Normann 2018; Jentzsch 2014) or the rejection of marketing purposes in favor of research purposes (e.g., Cvrcek et al. 2006; Danezis et al. 2005), our study reveals that, in the context of data-selling platforms, a number of so far hardly researched antecedents of individuals' willingness-to-sell personal information affect individuals' WTS: the company's origin and the level of security are antecedents that have not received attention in prior studies investigating the monetary valuation of personal data. These need to be considered in future studies that seek to better understand individuals' WTS on data-selling platforms.

Our qualitative study has resulted in a comprehensive framework of 12 inductively derived antecedents that affect individuals' willingness-to-sell personal data on data-selling platforms. One strength of our study is the usage of an inductive approach in order to identify antecedents that are relevant for users when assessing the value, they attach to their personal information. These antecedents should be considered by future studies investigating WTS on data-selling platforms.

Our second contribution concerns the relative weights individuals assign to a subset of factors identified in the qualitative study. One important finding emerged within the design phase of the conjoint analysis: Based on additional interviews, we identified three knock-out criteria for potential users of data-selling platforms: no transfer to third parties, the right to be forgotten, and one-time deals as duration of disclosure. Thus, these antecedents seem to act like inhibitors (Cenfetelli 2004; Cenfetelli and Schwarz 2011), with the power to impede that Internet users are actually willing to sell their data. Therefore, these antecedents should be handled with particular care in future WTS studies. Further, we identify the amount of compensation being the most important factor in this context, followed by the type of data, as well as the origin and legal framework of the intermediary and the purpose of use. Less important were the form of compensation and security. Future studies investigating individuals' WTS in the context of data-selling platforms should be aware of these differences in importance, if they focus on specific antecedents.

Moving beyond theoretical implications, our study also has practical implications for data-selling platform providers, customers, and buying companies. For data-selling providers we offer a list of key factors and inhibitors which should be considered when designing data-selling platforms. We also provide the relative importance for six of these antecedents and insights about potential manifestations. Based on the utility changes and monetary equivalents, we provide findings about possible pricing strategies for such platforms by representing monetary increases or decreases of the changes between different configurations. Further, our study illustrates how the most preferred data-selling platform would look like from the users' perspective. Taking into account the factors we have identified, providers can purposefully affect individual's willingness-to-sell personal information and facilitate adoption of their platforms. As a result, users of these platforms would be able to play a more active role in the data trading process which might result in increased fairness perceptions. For buying companies, it is important to note that the compensations should be adequate, and that Internet users dislike the sale of address data for the purpose of advertising most.

Limitations and Future Research Suggestions

Finally, let us note our limitations as well as potential future research directions. First, the innovative nature of data-selling platforms' business models and their underlying premise of trading personal information present a new idea for most individuals. In our study, we had to describe the functionality of these platforms to the respondents of our studies, for which we relied on mockups. These are less realistic than existing websites. However, hypothetical scenarios are a common practice in research (e.g., Malhotra et al. 2004) and due to these mockups we were able to exclude variation in functionality, branding, and marketing of different platforms and focus on aspects that were really relevant for our study. However, in future research studies, this restriction can be addressed by considering a real platform as research object.

Second, we collected the data in a Western European Country and, thus, lack a comparison of the findings between different countries. In other cultural samples, there might be additional factors that could have an impact on the willingness-to-sell personal information on data-selling platforms and the relative weights among these factors might vary as well. Consequently, future research could repeat this study with an intercultural sample, which would be of particular interest, as our results already reveal, that the origin of the platform and its legal framework are indeed important for the Western European participants. It would be interesting to see how a non-European sample would rate the different options with respect to the platform's origin.

A third limitation concerns the necessity to exclude some of the 12 antecedents identified in the qualitative study due to methodological requirements, for example the buying companies. The fixation to the general partner companies bears the risk of confounding effects due to different conceptions about the buying instances. Likewise, although we have carefully selected the attributes of the conjoint analysis, it cannot be guaranteed full independence. We therefore invite other researchers to take our results as a basis in order to conduct further studies on data-selling platforms. We advocate that this context should be of particular interest for researchers who are interested in the value of personal information due to its dedicated natural purpose of selling personal information. Our results help to understand the multitude of antecedents influencing Internet users' willingness-to-sell personal information in this context and can serve as a starting point to further investigate WTS.

Conclusion

As data-selling platforms are purely designed for buying and selling personal information, they can serve as a very natural research context to investigate the monetary value users attach to their personal information and their antecedents. Therefore, we conducted a two-step study in order to identify antecedents of willingness-to-sell personal information on these platforms and investigated the relative weights Internet users assign to a subset of these antecedents. Our study resulted in 12 antecedents which account for individuals' willingness-to-sell their personal information on such platforms. We identify three of them being knock-out criteria, meaning that potential users of such platforms would request their existence in the reported magnitude. Further we identify the amount of monetary compensation as the most important factor, whereas the respondents perceived security as less important. For research, we provide a comprehensive overview of antecedents for willingness-to-sell personal data on data-selling platforms highlighting the multitude of factors affecting the price of personal information in this context. For practitioners, we hint at important factors that need to be considered when designing data-selling platforms that should attract a higher user-base and diffuse as a new business model.

5 Research Paper 1.C: Distributive Equity Perceptions of Data-Driven Services

Title: Why Free Does Not Mean Fair: Investigating Distributive Equity Perceptions of Data-Driven Services

Authors: Wagner, Amina; Wessels, Nora; Brakemeier, Hendrik; Buxmann, Peter

Published in: International Journal of Information Management (59), 2021
<https://doi.org/10.1016/j.ijinfomgt.2021.102333>

Abstract

Individuals are supposed to perform a privacy risk-benefit analysis when deciding to transact with a free data-driven service provider. Building on equity theory, this article suggests that users incorporate the net value for providers in their trade-off. Based on two pre-studies and an experimental survey study among 200 free data-driven service users, we provide evidence that users' balance their own net value (benefits minus risks) as well as providers' net value from monetizing users' data. This leads to distributive equity perceptions which, in turn, affect users' satisfaction with the service and thus long-term success of the user-provider-relationship. In this vein, a distributive equity scale for the context of data-driven services is developed. Implications for research, providers and users are discussed.

Keywords: Information Privacy, Equity Theory, Distributive Equity, Free data-driven Business Models, Value of Data

Introduction

Establishing an image of fairness is the key to long-term success of companies (Seiders and Berry 1998). Furthermore, it is a major antecedent for user satisfaction and continuance intention (Herrmann et al. 2007; Joshi 1989). Especially free data-driven service providers like social networking sites (SNS) or any application relying on users constantly releasing personal information should focus on a fair value provided to them (Chou et al. 2016). Thus, appearing and being perceived as a fair partner is essential for providers. However, many users feel unfairly treated (Culnan and Armstrong 1999; Culnan and Bies 2003), which is exemplified by a study from the research institute SYZYGY revealing that only 27% of Americans perceive it as fair that Google and Facebook use personal data for targeted advertising (SYZYGY 2018). Moreover, another study by Orange indicates that only 6% of the surveyed users perceive that they benefit the most from revealing their data (Orange 2014).

So far, several factors have been found to account for a successful exchange relationship between users and online service providers (Chiu et al. 2009; Sierra and McQuitty 2005). A key recurring scheme in Information System (IS) research has been that users perform a trade-off with personal benefits and risks (Laufer and Wolfe 1977) when deciding to transact with a provider. Referred to as the privacy calculus, this perspective is intrapersonal in nature, as users purely assess their own rewards and losses (Culnan and Armstrong 1999).

Contrary, established service marketing literature building on equity theory has accumulated that customers evaluate not only their own net value, but also the net value of the service provider relative to their own (Oliver and Swan 1989; Ruyter and Wetzels 2000; Seiders and Berry 1998). They challenge the one-sided focus on intrapersonal benefits and risks assuming that customers compare their own net value with the net value of the service provider which in turn leads to an equity judgement. In other words, individuals weigh their net outcome (i.e., service benefits minus costs) against the net outcome of their exchanging partner and their subjective evaluation will become the basis of their distributive equity perception (Adams 1965). In this vein, customers are concerned about the distribution of outcomes. Against the background of equity theory as applied in service literature (Oliver and Swan 1989; Seiders and Berry 1998; Martinez-Tur et al. 2006), our study addresses the following research questions: *Are individuals concerned about the distribution of values between them and a free data-driven service provider? And if so, how does it affect distributive equity perceptions and thus satisfaction and continuance intention?*

Building on equity theory, current literature in the discourse of users' perception of free data-driven service providers is limited in several ways. First, a great body of privacy literature applies fairness literature as theoretical lens in an effort to explain various behaviors and outcomes (Son and Kim 2008, Turel et al. 2008, Zhou 2013, Krasnova et al. 2010b). However, they have paid little attention to the antecedents of fairness perceptions. Additionally, privacy research was rather concerned with the data handling and transfer process in terms of privacy issues while neglecting the monetary value of personal information and its distribution between users and providers (e.g., Xu et al. 2005; 2011a). Thus, privacy scholars treated the data exchange process between users disclosing their data and the service provider as a unidirectional flow of value, focusing on users' value only. This is not in line with equity theory, which proposes that instead of solely basing their attitudes on consequences arising for themselves, individuals also consider factors that do not affect themselves but providers (Adams 1965; Homans 1958). Furthermore, as users are concerned about equity in exchange relationships (Martinez-Tur et al. 2006; Oliver and Swan 1989), the maldistribution of values and its impact on fairness perceptions needs to be examined.

To answer our research questions, we conducted a three step approach. In two consecutive studies, we validated and pretested a self-developed distributive equity scale for the free data-driven service context. Within the main study - the experiment -, we present 200 Facebook users different monetary values with regard to how much money Facebook earns with their individual profiles to investigate their distributive equity assessment.

By providing a novel perspective on the relationship between users and free data-driven service providers as a bidirectional flow of value which leads to an interpersonal assessment of benefits and risks on an individual level, we offer several theoretical and practical contributions. Gaining deeper understanding of users' distributive equity perceptions and exploring its effects on satisfaction and continuance intention, we can help free data-driven service providers to carefully commensurate their users in order to promote long-term business success. Besides these practical implication, we reconceptualize users' intrapersonal trade-off between benefits and risks by incorporating an interpersonal perspective. Thus, we respond to a call from Dinev et al. (2015) to uncover and explore other dynamics within the privacy domain and integrate literature from related research fields. We further contribute to research on free data-driven services by highlighting the importance of distributive equity. Fairness with regard to how value is distributed between providers and users of free data-driven services has not been considered in research to date. Based on our knowledge, we are the first to integrate the concept of distributive equity in a research model and show how it impacts users' perceptions of such service providers. To conclude, it is not the data handling per se which needs to be fair, it is the level of compensation relative to the partner handling with the respective data.

Theoretical Background on Users' Assessment of Free Data-Driven Service Providers

Even though free data-driven services are in the center of attention in today's research projects, there exists no established definition of it. This might be due to the variety of services which free data-driven companies provide. They range from navigation systems like Google Maps to communication tools like Instagram. However, what they all have in common is that "its core business requires digital data" (Engelbrecht et al. 2016, p. 5) and that its services are offered without any monetary costs for users (Eling et al. 2016).

Users' attitudes towards free services and providers have been investigated from different theoretical perspectives. The majority of research on attitudes towards free data-driven services is based on social exchange theory and more particularly on the privacy calculus framework (Brakemeier et al. 2017; Krasnova et al. 2010a; Xu et al. 2009). Among others, social cognitive theory (e.g., Turel 2015), social capital theory (e.g., Ellison et al. 2007; MaksI and Young 2013; Valenzuela et al. 2009) and uses and gratifications theory (e.g., Chiu and Huang 2014; Sutanto et al. 2014) have been applied.

All these theoretical perspectives share one common characteristic: They assume that individuals' attitudes towards free data-driven service usage and providers are resulting from an assessment of a cost-benefit analysis taking into account the positive and negative consequences for users (Keith et al. 2013; Krasnova et al. 2010a; Li 2012). For example, in social exchange theory, social costs and benefits resulting from social interactions are weighted against each other and in turn influence social behavior. Studies employing privacy calculus theory focus on privacy risks and privacy concerns as negative outcomes, that are weighted against the benefits of using services when forming usage intention decisions (Bélanger and Carter 2008) or more specifically information disclosure intentions (e.g., Krasnova et al. 2010a). Uses and gratifications theory

investigates in how far online services can provide benefits in terms of gratification and social capital theory is concerned with the degree to which these services are beneficial for users in terms of relationship building. In the study employing social cognitive theory, behavior is influenced by benefits like satisfaction with the service and costs of using it reflected by feelings of guilt (Turel 2015).

Besides these benefits and risks investigated in prior studies, equity theory incorporates providers' net value from an individual perspective (Leventhal 1980). Equity theory (Adams 1965; Homans 1958) is applicable in so-called social exchange relationships. Within those relationships two parties interact with each other in such a manner, that value flows from one party to the other and this flow is accompanied by another flow of value in the opposite direction. In service research, the parties involved are usually customers and firms (e.g., Oliver and Swan 1989; Martinez-Tur et al. 2006). In transactions between these parties, customers invest inputs, oftentimes in terms of money, to receive some kind of service (Martinez-Tur et al. 2006). Thus, value in terms of money is flowing from customers to firms, while some intangible product represents the value flowing from firms to customers (Alter 2009). The assumption behind this is that the payment from the user to the company corresponds to the company's profit growth (i.e. the benefits for the firm). In a traditional service setting, the cost of the user corresponds to the benefit of the company. What sets free data-driven services apart from traditional services is that their users usually do not pay providers for these services, which means there is no obvious flow of value in the other direction (Eling et al. 2016).

However, what is often overlooked is that while they are used, free data-driven service providers gather and store personal information about their users (Gerlach et al. 2015; Kane et al. 2014; H Krasnova et al. 2012). Revenue is generated by allowing third parties to contact potential customers via their provided channels and thereby improve the targeting of their advertising (Heimbach et al. 2015; Iyer et al. 2005) and in turn personal information disclosed by users represents a valuable asset for free data-driven service providers (Feijóo et al. 2014). The relationship between free data-driven service providers and their users is therefore characterized by a bidirectional flow of value: (1) a flow of value in terms of services offered by the free data-driven service providers, which represent benefits for the users and (2) a corresponding flow of the user's personal information to the free data-driven service provider. The second flow is assumed to have a different value for the user in terms of privacy and the provider in terms of a monetary asset (C. Li et al. 2014). As both parties receive some kind of value from each other, the relationship between users and free data-driven service providers can be conceptualized as an exchange relationship as defined by equity theory (Clemons 2009; Cropanzano 2005). The perception of value distributions will then lead to an assessment of distributive equity, as proposed by equity theory (Adams 1965).

Equity theory suggests, that customers expect reciprocity in this exchange (Martinez-Tur et al. 2006), which means that they relate their own outcomes to the outcomes for the firm and thereby form a perception of distributive equity.

Under the umbrella of fairness in general, reciprocity has also been addressed in IS research. However, this research stream is unanimously concerned with data handling procedures and its trustworthy communication (Culnan and Armstrong 1999; Krasnova et al. 2010b; Son and Kim 2008). Their arguments are based on so called exchange fairness. It refers to users' assessment about whether the information is collected fairly and will subsequently be used fairly (Culnan and Bies 2003). For instance, Son and Kim (2008) conceptualized fairness as the treatment of personal information whereas Li and Sarathy (2007) referred to it as "the degree to which the data

requested appear relevant or appear to have a bearing upon the purpose of the inquiry”. While focusing on the data procedures, previous studies hypothesized a direct relationship between fairness and privacy risks. Beyond that, Malhotra et al. (2004) presented the dimensionality of privacy beliefs resulting from fairness perceptions. Therefore, privacy risks are often used as a proxy for a fair data exchange process (Culnan and Armstrong 1999; Li 2012). This implies that when companies promote to fairly treat their customers’ data, the perceived privacy risks can be lowered. This might be true in the case of data handling procedures and its communication, but does not hold for distributive equity as being a result of a perception between own benefits and risks relative to the outcome of the exchange party. In this case, users are concerned that they might be exploited by their exchange partner in terms of their overall outcome. They stipulate to be assured that efforts have been devoted to compensate them fairly taking into account the potential privacy loss they perceive. To sum up, fairness (i.e. equity) with regard to how value is distributed between providers and users of free data-driven services as assumed in equity theory has not been considered in IS research to date.

Conceptual Model and Hypotheses Development

According to equity theory (Adams 1965) users should weigh up the outcomes resulting from free data-driven service usage for themselves against the outcomes emerging for the free data-driven services provider when assessing providers’ distributive equity. This distributive equity assessment has, in turn, an influence on user’s general satisfaction with the free data-driven service provider and behavioral intentions in terms of continuance intention (Oliver and Swan 1989). Being satisfied with the exchange relationship leads to a higher degree of continuance intention (Chen and Chou 2012; Turel 2015). Figure 4 shows the conceptual research model which will be described in more detail along with its hypotheses development in the following paragraphs.

Commencing with users’ net value from transacting with a data-driven service provider, it builds on a benefit-risk analysis (Oliver and Swan 1989). It delineates an intrapersonal tradeoff between

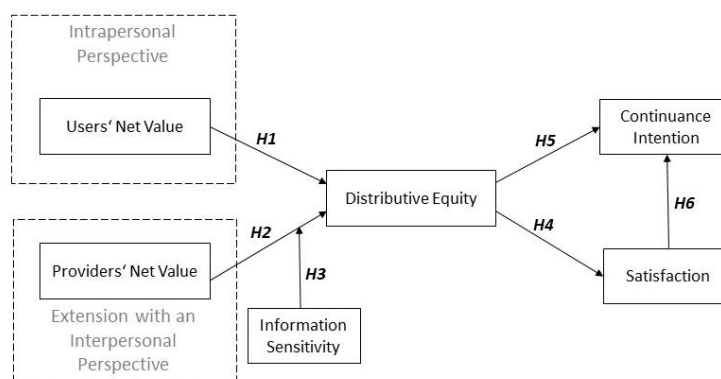


Figure 4. Conceptual model.

own benefits and risks based on the privacy calculus model (Dinev and Hart 2006). A multitude of benefits resulting from free data-driven service usage have been investigated in literature (Abramova et al. 2017; Wang et al. 2016). For instance, scholars have found that enjoyment (Krasnova et al. 2010a) as well as self-enhancement (Wagner et al. 2018c) fare major antecedent of self-disclosure on SNS. To receive benefits, users of free data-driven services are releasing their personal information. Thus, we build on the established assumption that users “pay” with their personal information online (Culnan and Armstrong 1999; Dinev and Hart 2006). Based on the

assumption of privacy research, releasing personal information to a provider comes with privacy risks - the expectation of losses stemming from privacy exposures (Smith et al. 2011). Privacy risks can thereby be defined as the sacrifice users make to be able to use the service provided (Dinev and Hart 2006; Xu et al. 2011a). The more favorable the tradeoff between benefits and privacy risks is for the user and thus the larger the net value from this user-provider-relationship, the fairer will the service provider be perceived by a user (Oliver and Swan 1989; Xia et al. 2012). In line with this reasoning, we formulate the following hypotheses:

H1: The higher users' perceived net values, the higher distributive equity perceptions of free data-driven service providers.

Users' net value "...is viewed as a sum of deservingness" (Joshi 1989, p. 345) which is further used as a benchmark to compare it to provider's net value. Therefore, we now turn to the value for the free data-driven service provider as this is the second factor influencing distributive equity perceptions of customers (Oliver and Swan 1989).

In literature on service in general and price fairness specifically (Seiders and Berry 1998; Xia et al. 2012), customers usually compensate providers of products or services with money. These payments then constitute the value firms receive. However, as argued above, in the free data-driven services marketplace it is not money that is transferred from users to providers but personal information (Bauer et al. 2012), which has no fixed value per se (Spiekermann et al. 2015a). An approach to resolve this problem is to consider the monetary value firms receive in transactions with third parties based on their users' data as the benefit they generate from the user-provider relationship. This is in line with studies investigating users' price fairness perceptions (Frey and Pommerchne 1991; Xia et al. 2012). In these studies, the revenue gained from selling a product is considered as the outcome of the company (Xia et al. 2012). Thus, when personal information is transferred, the equivalent would be the revenue a provider makes based on a user's personal information. Hence, assuming constant values for users, the higher the profit of the provider, the lower and therefore unfavorable is the ratio between the users' value from free data-driven services usage and the value received by the free data-driven service provider. Resulting from this, the net value of their exchange partner determines the perception of what individuals feel what they deserve (Franke et al. 2013). As net values should be commensurable, equity can be facilitated by a strong sense of reciprocity. If users feel exploited, then unfairness exists (Adams 1965). Providers' net value should therefore be negatively related to perceptions of distributive equity of the free data-driven service provider, as depicted in the following hypothesis.

H2: The higher the perceived net value of free data-driven service providers, the lower distributive equity perceptions.

Privacy research suggests that information sensitivity plays a dominant role in privacy judgements (e.g., Bansal et al. 2010; Malhotra et al. 2004). Information sensitivity describes the degree to which users perceive their disclosed information as being identifiable and thus privacy sensitive in nature (Bansal et al. 2010). This implies, the higher the perceived sensitivity, the greater the perceived loss of control over the handling of this data from a user perspective (Mothersbaugh et al. 2012). Most users, however, are unsure how providers handle and thus monetize their data (Schomakers et al. 2019). They only have a vague idea. We therefore assume that the higher the perceived sensitivity of the information, the more a user concentrates on the monetization process of his/her data in order to mitigate their own risk of losing control over their sensitive data (Mothersbaugh et al. 2012). The revenue for the provider based on the

individual user information gives the user an indication of how the data is being commercially handled. Therefore, we assume that users who perceive their information as being highly sensitive have a higher disposition to providers' value. The hypothesis is formulated accordingly:

H3: The relationship between provider's value of personal information and distributive equity is moderated by information sensitivity.

Additionally, equity theory suggests that distributive equity is a necessary condition for satisfaction (Oliver and Swan 1989), which is defined as the "contentment of the customer" regarding the provider's service (Anderson and Srinivasan 2003). Equity is even claimed to be the major determinant of customer satisfaction (Fisk and Coney 1982; Huppertz 1979; Zhu and Chen 2012). When users have positive experiences within a relationship, because values are distributed fairly, they are satisfied with the relationship. Generally, the more generous the provider compensates its users, the more favorably will users form their judgements about the former (Kuo and Wu 2011). In contrast, violations of fairness principles raise concerns about exploitation which leads to a lower level of satisfaction (e.g., Herrmann et al. 2007; Zhu and Chen 2012). This relationship between distributive equity and satisfaction has already been shown in different contexts like buyer-salesman exchanges (Oliver and Swan 1989), restaurant-guest relationships (Martinez-Tur et al. 2006), and organization-employee contracts (McFarlin and Sweeney 1992). Transferred to the context of free data-driven service providers, we hypothesize:

H4: The higher users rate free data-driven service provider's distributive equity, the higher is their satisfaction with the provider.

Distributive equity has also been shown to directly affect behavioral intentions (e.g., Yieh et al. 2007). In an exemplified study, Kaura et al. (2015) evidenced that equity with regard to perceived price fairness leads to a higher customer loyalty in the banking context. Building on these results, we hypothesize:

H5: The higher users rate free data-driven service provider's distributive equity, the higher is their continuance intention.

Satisfaction plays the predominant role in users' intention to continuously transact with a service provider (Bhattacharjee 2001). While satisfied users intend to continue using a service, dissatisfied users do not intend to use it in the future. This has also been shown in the context of free data-driven service providers (e.g., Chen and Chou 2012; Turel 2015; Udo et al. 2010). Accordingly, we hypothesize:

H6: The higher users are satisfied with free data-driven service providers, the higher is their continuance intention.

Methodology of the Multi Study Approach

The following chapter provides an overview of the applied methodology and describes the structure of our multi study approach consisting of two pre-studies and a main study. To test the research model presented above, we conducted an experimental study among Facebook users with a between-subject design, where we presented participants different monetary values about how much Facebook earns with their individual profiles to elicit either fair or unfair perceptions. For this purpose, we have implemented a Facebook Web App. Subsequently, participants were asked to answer a questionnaire to investigate their distributive equity assessment. Since existing scales stemming from traditional service research are not applicable to the context of free data-based services, as shown in the Appendix 1, we had to develop a new scale and validate it prior to

the conduction of the main experimental study. The scale development and its validation is described in section ‘pre-study 1’ as well as a pre-test of the values used for the experimental manipulation, are presented in section ‘pre-study 2’. Figure 5 visualizes the whole research process.

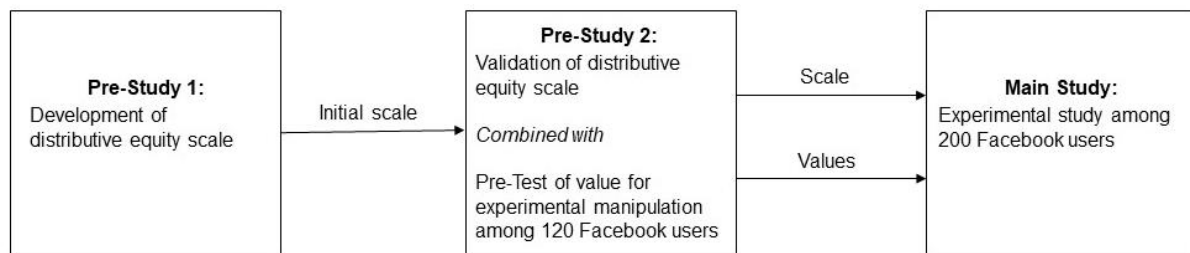


Figure 5. Multi-study approach.

We chose Facebook as our research site because of its high daily user base of 2.23 billion on average (Statista 2017a). Additionally, it is a good example for a free data-based service that has often been applied for user studies in IS research (Bauer et al. 2012; Turel 2015). Further, all Facebook users reveal personal information, resulting in individual profiles. This personal user information is the basis on which Facebook makes its profit. Due to its medial omnipresence, users are aware of this profit-making on the base of personal data.

Pre-Study 1: Scale Development

As existing distributive equity scales in the context of free data-based service providers focused on the distribution of users’ benefits and risks and established scales from service literature do not incorporate privacy risks, an appropriate scale for distributive equity had to be developed. Indeed, well-established scales (e.g. Son and Kim 2008, Krasnova et al. 2010b) confine to the privacy perspective and they only focus on what users give and get out of the service, where else we extend that perspective to an assessment of the relationship also considering what the provider obtains. This former assumption might be applicable for fee-based services where the payment of the customer is equivalent with what the provider receives as a benefit from this exchange relationship, but in terms of free data-based service providers the value user transfer to the provider is not equivalent to what the provider receives. Appendix 1 summarizes the former distributive equity/fairness scales in the privacy context with whom it was not possible to cover our re-conceptualization based on equity theory. Consequently, it was necessary to develop and validate a new distributive equity scale for our study. To do so, we followed the approach of MacKenzie et al. (2011).

The first step is the development of a conceptual definition of the construct (MacKenzie et al. 2011). MacKenzie (2003) postulates that “good definitions should (a) specify the construct’s conceptual theme, (b) in unambiguous terms, (c) in a manner that is consistent with prior research, and that (d) clearly distinguishes it from related constructs” (MacKenzie 2003, p. 325). Complying with this advice, we iteratively improved our definition, while steadily strengthening the description to write as clearly and exact as possible (Churchill 1979). Finally, we defined distributive equity as “the degree to which a user perceives the exchange between him/herself and a service provider as fair given the extent to which each party profits from the relationship.”

Building on this definition, a team of 4 privacy researchers generated 15 item proposals pursuing full coverage of all substantial domain aspects of our distributed equity construct. Here again, we took care of precise, clear, and simple wording (Podsakoff et al. 2003). To evaluate the item’s

content validity, MacKenzie et al. (2011) recommend an approach building on Hinkin and Tracey (1999) and Yao et al. (2008), which we applied for the assessment of our items: In this regard, we conducted a study asking 13 Information System researchers to evaluate our items in comparison to the former distributive equity items from Son and Kim (2008). We created a matrix consisting of our and the other definition of distributive equity in the top of the columns and listed the items of the two constructs in a mixed sequence in the rows. The raters were asked to evaluate on a 5-point Likert scale ranging from “not at all” to “completely” the extent to which each item covers the defined construct domains. By integrating another construct, we ensure that the new items are free of content from extraneous domains (Schriesheim et al. 1993).

Based on the researchers’ assessments (8 females and 5 males), we conducted a one-way ANOVA with repeated measures to test for every single item whether its mean rating on the dedicated construct’s domain differs from the same item’s ratings for the other distributive equity definition (MacKenzie et al. 2011). Based on the ANOVA-results, we could identify seven items that were rated to resemble our construct significantly as its mean values for the newly developed construct were significantly different compared to the mean ratings of the other construct ($p < 0.05$). The consent of these final items was in general very high with a rating of 4.38 on average. Other items like “The profit the firm generates with me is adequate.” were rated comparable low with a mean consent of 2.32 and were thus removed from further testing.

Pre-Study 2: Scale Validation and Experimental Manipulation

Continuing the procedure of MacKenzie et al. (2011), we validated the developed initial distributive equity scale (7 items) and combined this with a pre-test of the profit per Facebook profile needed for the experimental manipulation.

For the validation, we do not only show the manipulation values: According to the call for more realistic study designs by Dinev et al. (2015), we aspired after a more credible manipulation close to reality as fairness impressions rather emerge in tangible situations. Thus, we implemented a Facebook Web App, which told participants that it is able to estimate the revenue Facebook generates with their profiles. The app was structured as follows: After an introductory page, telling the app can calculate Facebook’s profit based on individual profiles, participants of the study were asked to type in their user name and password in the app to login to Facebook. Subsequently, a spinning wheel symbolized the value calculation in the background. Afterwards, we presented the participants different values about how much Facebook earns with their individual profiles (see Figure 6) and let them fill out the 7-item self-developed distributive equity scale. With regard to Facebook’s revenue, we decided to pretest four values. Half of the participants got high values (98 Euro or 198 Euro), and the other half low values (38 Cent or 9 Euro) in order to gain fair and unfair sentiments and therefore be able to build variance. Those four values have been obtained by asking 24 Facebook users (mean age: 31.12) to estimate the threshold of the revenue Facebook gains based on their individual profile (1) which would be lower than expected and (2) surprisingly high. Taking the bottom and the top quartile of each stated amount among all respondents, we were able to receive 4 amounts which were pretested in study 2. We decided to present the values and not to let the participants guess the profit as Facebook does not release any information about their profit based on individuals’ profiles and, thus, it could be complicated for the participants of the study to estimate a value. Furthermore, due to the high and low values, we can elicit either fair or unfair perceptions. Figure 6 shows the screenshot of the Facebook app presenting 98 Euro as an example.



Figure 6. Screenshot of the Facebook web app.

In total, 120 students completed the scale and amount validation test. On the basis of this assessment, we conducted an exploratory factor analysis as suggested for the pre-test by MacKenzie et al. (2011) and could finally validate five items, as their factor loadings were higher than the two dropped out items which fall below the threshold of 0.7 (Hair et al. 2011). The final list of items can be found in Appendix 2. Further, we could identify 38 cent as solid low and 98 Euro as high borders because they evoke clear fair and unfair distributive equity perceptions and thus serve as a solid manipulation for our main experiment. 9 euros was perceived as neither fair nor unfair and 198 euros did not differ from 98 euros in individual's distributive equity perceptions as both values tend to be perceived as unfair. Supporting our argumentation for 98 euros, it is closer to Facebook's true average advertisement revenue per user per year of \$30 (Statista 2020c) by the time of conducting the study.

Main Study

On the basis of both pre-tests, we started to empirically test our research model by conducting an experimental online study among Facebook users. We distributed a short description of the study and the hyperlink of the questionnaire via several Facebook groups, lecture panels, and by spreading flyers on the campus. To incentivize the participants, they had the chance to win one 50 Euro and five 10 Euro gift cards of two big online retailers. To counteract common method bias (Podsakoff et al. 2003), we encouraged participants to type in their answers spontaneously and honest as there are no right or wrong answers.

At the beginning of the study, some general demographics were measured, like gender, age, and usage frequency of Facebook as well as active use as control variables. Participants who were identified as Facebook users were forwarded to the Facebook Web App. Randomly, either 38 Cent or 98 Euros were presented as Facebook's yearly profit based on each individual profile. Afterwards, the participants were forwarded to the questionnaire where all main constructs of the study were presented.

In addition to the self-developed distributive equity scale and the manipulated net value for providers' from personal information, we used established scales from prior literature for all other main constructs. For the measurement of users' net value, we adapted a scale from Krasnova et al. (2010b) consisting of three items. It measured users' fairness perception based on an intrapersonal valuation of perceived benefits minus privacy risks. Satisfaction was measured with four items developed by Hu et al. (2015) and a scale of Lankton et al. (2015) was used for the continuance intention measurement. Information sensitivity was measured with 3 items from Bansal et al. (2010) based on a semantic differential ranging from "not sensitive at all" to "very

much sensitive". To control for the rather low or high perception of providers' net value, we measured participants' disconfirmation based on Bhattacharjee (2001) regarding the presented revenue. Controlling for disconfirmation is important, because it is central for customer satisfaction (Martinez-Tur et al. 2006; Bhattacharjee 2001) and it shows whether our manipulation was successful. Apart from providers' value and information sensitivity, all other constructs have been measured on a 7-point Likert scale ranging from "strongly disagree" to "strongly agree". Appendix 2 lists all items of our research model. Following the advice of Meade and Craig (2012), we also included an instructed response item for identifying careless responders. Further, we included a second manipulation check (i.e., an open-ended question) in the questionnaire by asking which value the Facebook Web App has presented to the respondents.

Results of the Main Study

Overall, 337 Facebook users participated in our survey. All participants who did not take part in the manipulation meaning that they did not log in to their profile to see how high Facebook's revenue is have been removed. All participants passed the manipulation check. This resulted in 200 observations that were used for all further analyses. Demographic information of our respondents can be found in Table 10 below. Compared to the actual Facebook user distribution in age and gender in western European countries (Statista 2017a), our sample represents the network population quite well. On average, our participants have got 358 connected friends on Facebook and use the site between 10 to 30 minutes per day.

Table 10. Demographic information of main study's respondents.

Gender	N	%	Education	N	%
Male	140	70	Basic Education	1	0.5
Female	60	30	Secondary Level Education	7	3.5
			Higher Education	192	96
Age	N	%	Employment	N	%
18-25	137	68.5	Student	154	77
26-35	56	28	Employed	38	19
36+	7	3.5	Other	8	4

Structural equation modelling was used to analyze our data. We used the variance-based PLS method implemented in SmartPLS (Ringle et al. 2015) over covariance-based methods like LISREL, because it is especially suited for theory development in early stages (Fornell and Bookstein 1982).

Before analyzing the structural model, we analyzed the validity of our survey instrument. To verify convergent validity, factor loadings of the items on their constructs as well as composite reliability of and average variance extracted by the constructs were investigated (Xu et al. 2012). An exploratory factor analysis with Varimax rotation was performed to obtain the factor loadings depicted in Appendix 2. All items showed loadings greater than 0.7 on the construct they were intended to measure, which indicates convergent validity according to Hair et al. (2011).

Composite reliability (CR) was larger than the proposed threshold of 0.7 (Bagozzi and Yi 2012) and also the average variance extracted (AVE) indicated convergent validity, as it exceeds the threshold value of 0.5 for all constructs (Hair et al. 2011). Cronbach's α values were also satisfactory as they exceeded 0.7 (Bagozzi and Yi 2012) for all constructs. Therefore, convergent

validity of our measurement model is given. For each construct, all values for Cronbach's α , CR and AVE as well as mean and standard deviation (SD) are provided in Table 11 along with construct correlations.

Table 11. Mean, Standard Deviation (SD), Cronbach's α (Cr. α), Composite Reliability (CR), Average Variance Extracted (AVE) and Construct Correlations.

Construct	Mean	SD	Cr. α	CR	AVE	CI	DE	SAT	IS	UNV
Continuance Intention (CI)	5.49	1.57	.970	.980	.944	.971				
Distributive Equity (DE)	3.883	1.75	.966	.973	.880	.369	.938			
Satisfaction (SAT)	3.58	1.48	.943	.959	.855	.523	.510	.925		
Information Sensitivity (IS)	3.05	1.31	.892	.931	.817	-.010	-.106	.104	.904	
Users' Net Value (UNV)	3.71	1.60	.882	.927	.810	.420	.530	.566	.409	.900

We proceeded by investigating discriminant validity. Discriminant validity first requires all items to load higher on the construct they were intended to measure than on any other construct (Bagozzi and Yi 2012). The results of our exploratory factor analysis given in Appendix 2 show that this criterion is met. Apart from factor loadings, discriminant validity requires the variance shared between each construct and its items to be greater than the correlations between the construct and all other constructs (Fornell and Larcker 1981). This is given when for each construct the square root of the AVE (diagonal elements in Table 11) is greater than the correlation with any other construct (Fornell and Larcker 1981). This second criterion for discriminant validity is also fulfilled.

As common method variance may be problematic in survey research, we followed the recommendation of Podsakoff et al. (2003) by running Harman's single-factor test. According to this test, common method variance is unlikely to be an issue if no single factor explaining the majority of covariance among the measures turns out in a factor analysis incorporating all measures in a survey. The most covariance explained by one factor turned out to be 35.2% in our data. Common method variance is therefore unlikely to be a problem in our study (Podsakoff et al. 2003). Additionally, we tested for common method bias by including a marker variable - the tendency to fantasize lend from Darrat et al. (2016) and also used in Son and Kim's (2008) study as a predictor for all endogenous constructs in our model. In doing so, no regression paths that were significant in the baseline model became insignificant. To conclude, common method variance does not seem to be an issue in our dataset (Rönkkö and Ylitalo 2011).

Additionally, we tested whether the means of disconfirmation (the revenue being higher than expected) significantly differentiates between the high and the low revenue group of respondents in order to demonstrate a successful manipulation. Based on a t-test in SPSS, we were able to show that the mean of the high revenue group (4.21) and the mean of the low revenue group (2.29) were significantly different.

After ensuring the validity of our measurement model, we now turn to the analysis of the hypothesized relationships as depicted in our research model. The standardized root mean square residual (SRMR) of 0.062 indicates good model fit as it is well below the threshold of 0.08 (Hu and

Bentler 1999). Predictive power is assessed in terms of variance explained in the endogenous variables by the model in PLS analyses (Chin 2010). R^2 values show that our model explains 41.1% of variance in distributive equity and 25.5% of the variance in satisfaction as well as 27.5% of variance in continuance intention.

A bootstrapping (Davison and Hinkley 1997) with 5,000 resamples was then performed to investigate the significance of path estimates. Our first two hypotheses, were concerned with user's and provider's net value from personal information and its impact on perceived distributive equity. We found both relationships to be significant for user's net value ($\beta=0.464$, $p=0.000$) and provider's net value ($\beta=-0.315$, $p=0.000$), hence supporting H1 and H2. In line with H3, the moderating effect of information sensitivity on the link between provider's value and distributive equity is also significant ($\beta=0.124$, $p=0.041$). Distributive equity positively affects satisfaction ($\beta=0.504$, $p=0.000$), while satisfaction leads to a higher continuance intention ($\beta=.444$, $p=.000$). However, we had to reject H5, because distributive equity is not significantly linked to continuance intention. A Sobel test statistic ($p=0.000$) confirmed that satisfaction fully mediates the above link (Baron and Kenny 1986). When satisfaction is added to the research model, the significant relationship between distributive equity and continuance intention disappears. Apart from H5, all hypotheses are therefore supported by our data. The signs of the path coefficients were in line with our hypotheses. All path estimates with indications of significance and R^2 values are given in Figure 7.

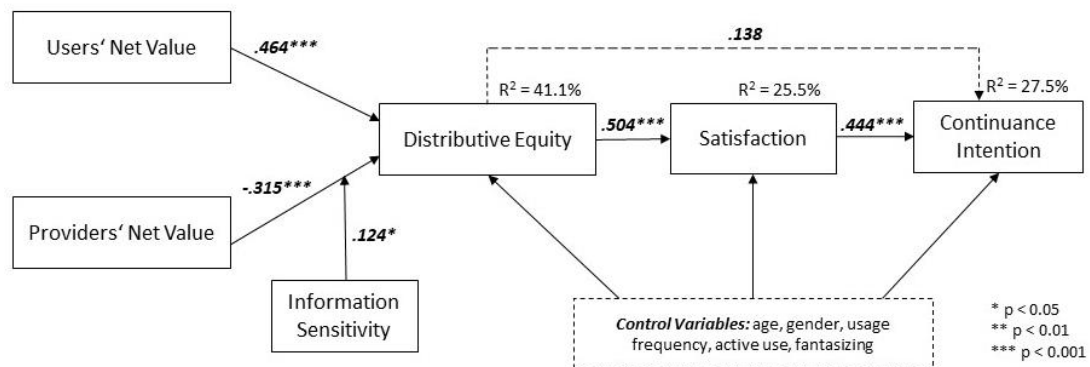


Figure 7. Results of the PLS analysis.

Besides, testing our main model, we also included control variables as influential factors for all dependent variables into our model and re-performed a bootstrapping with 5,000 samples. Active use was positively associated with satisfaction ($\beta=0.235$, $p=0.000$). Age, gender and Facebook usage frequency had neither a significant impact on distributive equity nor satisfaction or continuance intention.

Discussion

This study's goal was to shed light on distributive equity perceptions of free data-driven service users. In this vein, antecedents and cognitive as well as behavioral outcomes of distributive equity perceptions have been identified. The main research findings are synthesized in the next section and contrasted with existing work in this field. Theoretical and practical implications are discussed in the following sections.

Research Findings

Free data-driven services have been largely considered from a privacy perspective in extant research. This stream of research is concerned with the question under which circumstances Internet users are willing to have their personal information gathered and processed by service providers (Krasnova et al. 2010a, Xu et. al 2009, Dinev and Hart 2006). In this paper, we provide a new conceptualization of users' assessment of free data-driven services. Building on equity theory (Adams 1965; Homans 1958), we extend established research focusing on users' intrapersonal perspective stemming from the privacy calculus framework (e.g., Wang et al. 2016) by arguing that this conceptualization only provides an incomplete picture of the values resulting from free data-driven service use. Apart from the net value (benefits minus costs) for users, we also consider the value for the provider from a user perspective. The values exchanged are thereby represented by service benefits (transferred from providers to users) and monetizable personal information (transferred from users to providers). Specifically, we presume that users' perceptions of distributive equity regarding a data-driven service provider are not solely based on the outcomes of this exchange arising for themselves but also on what the provider gains from it.

We test this reconceptualization based on an experimental survey study among 200 Facebook users. With the help of a Facebook Web App, we presented our respondents two randomly assigned values Facebook gains from individuals' profile information and were thus able to raise either low or high distributive equity perceptions. Our study shows that users of free data-driven services indeed compare their own net value from using the service (the benefits minus the costs in terms of privacy risks) with how much the provider of the service earns out of the relationship. Particularly, a higher net value for the provider is negatively linked to users' distributive equity perceptions. These results confirm the established tradeoff between benefits and risks in privacy research and extend it by knowledge from offline service literature (Oliver and Swan 1989; Martinez-Tur et al. 2006).

Another interesting result of our study is that the relationship between provider's net value based on users' information and distributive equity is moderated by information sensitivity. Thus, users who perceive their information as being very sensitive have a higher disposition to provider's net value from personal information. Contrary, users who perceive their data disclosed on Facebook as being less sensitive pay a lower attention to the monetization extent of their personal information. This moderation effect supports the strong role of perceived information sensitivity previously shown with regard to users' perceptions of providers' data handling processes (e.g., Mothersbaugh et al. 2011).

Overall, our study provides evidence that the more money the provider of a free data-driven service generates based on the data provided by a user, the less equity is attributed to the service provider which, in turn, lowers satisfaction with the service and ultimately the intention to continue using the service. Even though Krasnova et al. (2010b) could not find that distributive equity perceptions are significantly linked to privacy-related judgements, we are able to show that distributive equity drives satisfaction with the service. Notably, since 2010 data-driven service users got more and more aware of the commodification of privacy and the underlying concept of paying with personal information to receive 'free' services in return. Moreover, distributive equity was measured on a high abstraction level which is comparable to the measurement of satisfaction. In this regard, we contextualized the distributive equity scale and show that it is more related to users' worry of the monetization extent of personal information instead of users' concern of losing

control over personal information as originally applied in privacy research (e.g., Son and Kim 2008).

However, what we could not find was a direct link between distributive equity and continuance intention. This may be due to the important role of satisfaction as a mediator which is in line with prior research (e.g., Chang and Chang 2010; Chiu et al. 2007).

Neither demographic variables (i.e., age, gender) nor Facebook usage frequency and active use turned out to be significantly linked to distributive equity. Controlling for these variables shows that distributive equity perceptions are robust against service-dependent influences. Apart from this main study, two pre-studies have been conducted in order to (1) identify two applicable net values which Facebook gains from personal information and to (2) develop a distributive equity scale according to the guidelines from MacKenzie et al. (2011). This self-developed distributive equity scale for the context of data-driven service providers goes beyond other available distributive equity scales which solely consider the value for the user but not for the provider (e.g., Zhou 2013, Turel et al. 2008). Theoretical and practical contributions are discussed in the following.

Theoretical Implications

Our study adds to IS literature in four ways. Our first and superordinate theoretical contribution lies in the reconceptualization of free data-driven services as an exchange of values between users and providers and thereby questioning the privacy-dominated discussion of this type of business models. Based on our reconceptualization we open the discussion to the area of service research. In particular, we provide arguments that free data-driven service providers need to commensurate their users as it constitutes an exchange relationship as applied in traditional service research. This reconceptualization and therefore new theoretical lens we apply for investigating free data-driven services may serve as a starting point for other research in the field of valuation of privacy or customer satisfaction in e-commerce helping to further clarify the dynamics of this type of business models.

Based on this overarching contribution, we see 3 subordinate contributions. The first subordinate contribution lies in the extension of the purely intrapersonal trade-off between perceived risks and benefits for the user traditionally applied in privacy research (e.g., Krasnova et al. 2010a; Li 2012). We conceptualize the usage of free databased service providers as a bidirectional flow of values. Thereby, we integrate the net value for the provider into our model by showing a negative correlation between the revenue the provider of a free data-driven service generates based on the personal data of a certain user. The provider's revenue is thereby compared to the net value the service creates for users. This net value created for users is the difference between the benefits and privacy costs which is also considered in IS privacy research. However, we extend this notion by showing that this net value is not only directly related to usage intentions, but it is also compared to what the provider gains from the business relationship between user and firm. If this relation becomes disproportionately positive for the provider, users react with reduced perceptions of fairness and in turn a lower satisfaction with the service provider. This lower satisfaction thus leads to a reduced intention to continue using the service.

We further contribute to privacy research by highlighting the importance of distributive equity for research on free data-driven services. Albeit the concept of fairness has also been addressed in extant research, this is unanimously centered on the procedures of data collection, handling and secondary data use (Culnan and Armstrong 1999; Krasnova et al. 2010b; Zhou 2013). Their arguments are based on so called exchange fairness. It refers to users' assessment about whether

the information is collected fairly and will subsequently be used fairly (Culnan and Bies 2003). Even though, different researchers found distributive equity to play the predominant role in predicting customers' attitudes towards a service provider (Oliver and Swan 1989; Martinez-Tur et al. 2006), we are the first to integrate the concept in a privacy research model and show how it impacts users' perceptions of such business models. Thus, it is not the data handling per se which needs to be fair, it is the level of compensation relative to the partner handling with the respective data. In this vein, we respond to a call from Krasnova et al. (2010b) to better understand fairness perceptions beyond data handling procedures.

Our results may also inform research based on the notion of privacy as a commodity. This stream of research assumes that individuals see their privacy as an economic good that can be traded for benefits (Acquisti et al. 2009; Krasnova et al. 2009b; Spiekermann et al. 2012). We extend this notion by arguing that the privacy given up by users has two different values: one for the users and one for the providers. The value of privacy for users is what has been extensively studied by IS privacy research (e.g., Acquisti et al. 2009; Huberman et al. 2005; Tsai et al. 2011). We extend this concept by introducing a second economic value that can be mapped to personal information: the revenue a service provider may generate based on it. This duality of values of privacy is particularly interesting against the background, that it separates traditional services from free data-driven services. In traditional service relationships, the price users pay (and therefore the negative value resulting from using a service) is equal to the gain of service providers (the positive value resulting from offering the service for providers). This equality does not hold any more when considering free data-driven services. The negative value represented by a loss of privacy does not necessarily equal the amount of money a service provider can generate based on that loss of privacy. Therefore, the notion of privacy as a commodity should be extended in so far, that privacy has not only an economic value for users, but also one for providers. These two economic values can, but do not have to be equal.

Beyond that, our results confirm the strong role of satisfaction as a full mediator between equity perceptions and intention in general (Chiu et al. 2007; Oliver and Swan 1989, Chang and Chang 2010). Distributive equity perceptions per se do not drive continuance intention, but they are mediated by satisfaction.

Practical Implications

Apart from these theoretical contributions, our findings can also inform providers of free data-driven services, its users as well as policy makers. Regarding perceptions of fairness, marketing research (Oliver and Swan 1989; Martinez-Tur et al. 2006) found that distributive equity is a strong predictor of customer attitudes towards firms. Therefore, our results show that providers should deliberately choose in how far they monetize user data. If user data is monetized too extensively and users become aware about how much money is generated based on their personal information, they might feel exploited if this value is not opposed by an appropriate value provided by the service. To ensure that user satisfaction does not suffer, business model innovations leading to enhanced monetization of user data should be accompanied by initiatives that compensate users. This can either be done by increasing the benefits the service provides to users as shown in our research model, but also other measures to increase customer satisfaction might help to prevent customers from service discontinuance. Otherwise, service providers might suffer from a decreasing user base and in the long-run severe financial problems.

Another factor that should be taken into consideration is that users oftentimes only have a vague feeling about how much money a firm generates based on their personal information. Indeed,

research investigating the value users assign to their personal information has shown very different results, depending on various factors that need to be considered, indicating that users are challenged stating a value (Wagner et al. 2018a). Being aware that free data-driven services might not be as “free” as it seems but being paid with the value of personal information might further influence user behavior. It seems plausible that users overestimate the monetary value of their personal information for firms (Huberman et al. 2005; Roeber et al. 2015). In this scenario, it might even be beneficial for firms to disclose the actual (lower) value generated based on this information to increase customer satisfaction. Thus, purposeful marketing and transparency regarding the actual amount earned with users’ personal information might positively influence distributive equity and satisfaction perceptions changing actual business practices. Especially, if users disclose very sensitive information to a provider, the value a provider generates based on user’s data is more heavily taken into account when making a distributive equity assessment. Therefore, service providers should focus on a moderate monetization of these users’ data, otherwise they might run the risk that their most valuable customers (who disclose sensitive data) will discontinue their usage in the future.

Finally, our results can motivate policy makers to monitor whether users perceive free data-driven services as being fair, because usage discontinuance of innovative services may hinder economic growth. As free data-driven services like Google, Facebook and others are one of the biggest public corporations which lead digital innovativeness, its user perception should be of heightened interest for governments.

Limitations and Future Research Suggestions

As with every empirical study, the findings of our research have to be considered in light of its limitations. The first limitation lies in the context we used to investigate our hypotheses. We deliberately chose Facebook users as our sample, because of its large user base and controversial media coverage regarding Facebook’s financial results. Although the relationships found in our research could also be applicable to non-SNS services monetizing user data, more research is necessary to provide according evidence.

A second limitation is that our results are based on empirical data obtained from free data-driven service users who were mainly students with a single cultural background. Research debates whether studies on free data-driven service users with different cultural backgrounds are comparable (Krasnova et al. 2012; Schomakers et al. 2019). More research is necessary to investigate samples with other cultural backgrounds and other education levels to confirm our findings.

Third, we only considered ex post equity perceptions of individuals that have already used this specific free data-driven service under investigation. Ex ante assessments of potential users are therefore unconsidered by our research. Future research efforts could thus investigate in how far assessments of distributive equity differ with regard to whether they are made ex ante or ex post. An additional limitation lies in the conceptualization of users’ and providers’ net value. Thereby, we did not measure the perception of costs and benefits for both sides on a more nuanced level. However, we additionally measured active Facebook use in order to control whether people who are interacting a lot with others on the platform perceive higher benefits and thus are more likely to evaluate the SNS as a fair.

Fourth, we had to conduct the study among users of a free data-driven service, which always carries the risk of a self-selection bias. Indeed, comparing both groups, deniers rate significantly higher on their general perceived privacy concerns than joiners ($p=.002$). So, even when less

privacy concerned users experience a lower degree of fairness due to the monetization of their personal information, it would even be worse for highly privacy concerned individuals.

Finally, our research goal was to investigate whether users of free data-driven services perform a trade-off between their own net value and the net value of the provider in order to make a distributive equity judgement. Therefore, we solely manipulated the net value of the provider with a rather low and rather high amount. In an attempt to identify a threshold at which free data-driven service providers are perceived as unfair, it might be fruitful for future research to conduct a contingent sensitivity analysis with varying amounts of revenue.

Conclusion

Most data-driven services are free of charge for its users. However, even though users do not transfer money to its providers in return for services, they are giving up their privacy by continuously releasing their personal information. This personal information is in turn used by data-driven companies as a basis for generating profit. Neglecting the bidirectional flow of values between users and providers of free data-driven services might lead to problems for providers, because a fair distribution of values is a necessary precondition for users' satisfaction with the service provider. Given that data-driven service providers gain profit based on their users' data, customers need to be commensurate with an equivalent flow of value. Establishing a fair exchange process can lead to a higher satisfaction and thus a successful long-term user-provider relationship.

6 Research Paper 2.A: Evaluability Bias in Privacy-Related Decisions

Title: When Risk Perceptions Are Nothing But Guesses – An Evaluability Perspective on Privacy Risks

Authors: Brakemeier, Hendrik; Wagner, Amina; Buxmann, Peter

Published in: International Conference on Information Systems (ICIS), Seoul, South Korea, 2017

Abstract

Traditionally, a majority of IS privacy research assumes that individuals are able to form confident privacy risk perceptions when being confronted with situations involving the disclosure of personal information. We challenge this assumption by offering theoretical arguments that privacy risks are difficult to evaluate for individuals. Based on an experimental survey study among 233 participants we show that (1) the formation of privacy risk perceptions is dependent on external reference information and (2) more external information allow a more confident risk judgment, which in turn has a stronger impact on an individual's privacy-related behavior. These findings extend privacy calculus theory by introducing the context-specific evaluability of privacy risks as a moderator of the effect of perceived privacy risks on usage intentions of privacy-invasive information systems. Theoretical and practical implications are discussed and future research suggestions are provided.

Keywords: Privacy Risks, Privacy Calculus, Evaluability, Confidence

Introduction

Suppose Jeff is scrolling through his smartphone's app store in search of a new task management app. His eyes wander through a long list of search results until he taps one that looks appropriate for his needs. Although there are not many, the ratings and reviews seem to be okay and the screenshots look promising. Jeff's finger hovers above the download button, but suddenly a section listing a variety of personal information stored on his phone catches his attention: In order to use the application, it requires Jeff to grant access to his contact list, calendar information and his phone's camera. Jeff pauses asking himself, whether there would be a high potential for loss associated with giving these information to the application provider. What Jeff just experienced is exactly what IS privacy researchers ask survey participants to do when measuring the perceived risks of information disclosure. Consider for instance the items used by Malhotra et al. (2004) to measure the perceived risks of information disclosure: They ask survey participants to indicate the extent to which they agree to statements like "There would be high potential for loss associated with giving (the information) to online firms" (Malhotra et al. 2004, p. 352) and "Providing online firms with (the information) would involve many unexpected problems" (Malhotra et al. 2004, p. 352). According to privacy calculus theory (Laufer and Wolfe 1977; Li 2012), individuals would then perform a rational tradeoff between the perceived risks of information disclosure and the perceived benefits of information disclosure to form their intention to use privacy-invasive information systems. However, although it might well be that Jeff came to a risk perception in terms of a vague feeling, he might not necessarily be sure that his risk judgment is valid. Thus, the question whether individuals are able to perform confident privacy risk tradeoffs arises.

Based on evaluability theory, we argue that most individuals just like Jeff are not able to evaluate risks inherently. It might rather be that they lack sufficient information as well as clear and stable internal preferences to form consistent opinions regarding the quality of product attributes in general (Creyer and Ross 1997) and privacy threats in particular (Dinev et al. 2015). Such product attributes are referred to as difficult to evaluate in evaluability theory (Hsee and Zhang 2010). When being confronted with objectively observable product attributes that are difficult to evaluate, individuals generally react insensitive to changes in the quality of these (Hsee et al. 1999). However, if provided with external reference information facilitating evaluation, sensitivity increases, because individuals have guidance in telling whether a certain manifestation of a product attribute is good or bad and as a consequence regard their evaluation of the attribute quality as more valid and therefore incorporate it more strongly in their decision-making (Hsee and Zhang 2010). Hence, the impact of a privacy risk perceptions should depend on how they were formed. To date, this potential coupling between the formation and impact of perceived privacy risks has not been considered in IS privacy research. However, if proven true, measurements of perceived privacy risks and their empirically observed correlations with behavioral consequences would be rendered incomparable due to differences in available reference information across studies. Therefore, we challenge the assumption that individuals are inherently able to form confident risk perceptions. Consequently, we question the basic assertion of privacy calculus theory that perceived privacy risks as measured in current research uniformly influence usage intentions of privacy-invasive information systems independently of how they were formed. Accordingly, we investigate the following research questions:

RQ1: Are users of privacy-invasive information systems able to evaluate the privacy risk associated with the disclosure of a certain amount of personal information independently?

RQ2: Do perceived privacy risks influence behavior differently when they are formed in conditions that facilitate evaluation compared to when they are difficult to evaluate?

By incorporating an evaluability perspective (Hsee and Zhang 2010) into the privacy calculus (Laufer and Wolfe 1977; Smith et al. 2011), we develop theoretical arguments that individuals react relatively insensitive to changes in the amount of data gathered by an information system, when they have to rely entirely on their “inner scale” and hinge on intuitive risk judgments when deciding whether to use a privacy-invasive information system. Only if reference information facilitating the risk judgment is made available, the amount of data gathered by an application affects risk perceptions and these are perceived as sufficiently substantiated to serve as decision-basis. We provide empirical evidence for these propositions based on an experimental survey study among 233 participants and thereby show that the presence of reference information significantly increases the effect of the amount of data gathered by a privacy-invasive application on the perceived risk of information disclosure as well as the effect of the perceived risks of information disclosure on the behavioral intention to use a privacy-invasive information system.

The remainder of this paper is structured as follows: We begin by outlining the theoretical background of our research in two steps: First, we discuss in how far the amount of data gathered by a privacy-invasive information system constitutes a difficult-to-evaluate product attribute. We then extend privacy calculus theory by proposing that the effect of the perceived risks of information disclosure on the intention to download an application depends on how risk perceptions were formed. Afterwards, we describe the experimental survey study we conducted to empirically test our deduced hypotheses and subsequently present our findings. We then discuss our findings, depict limitations of our study and propose promising future research opportunities. Finally, the paper closes with a conclusion.

Theoretical Background

The Evaluability of Personal Information Disclosures

IS privacy research is concerned with the reactions of individuals to privacy-invasive information systems (e.g., Dinev et al. 2006; Krasnova et al. 2012; Li et al. 2010; Xu et al. 2009). Privacy-invasive information systems refer to information systems that gather, store and process information about their users. As providers could use this information in unforeseen ways or share it with third parties, the use of a privacy-invasive information system is regularly associated with a loss of control about one’s personal information (Malhotra et al. 2004). This loss of control can propagate and persist for an unpredictable span of time (Acquisti and Grossklags 2003). Thus, the central property of privacy-invasive information systems is that using them is associated with potentially negative consequences resulting from a loss of privacy. This potential loss is captured by the concept of perceived risks of information disclosure and has been investigated as an antecedent to information disclosure and usage behavior in numerous studies (e.g., Fortes and Rita 2016; Krasnova et al. 2010a; Min and Kim 2015; Pavlou and Fygenon 2006; Sharma and Crossler 2014; Wang et al. 2016). Findings show that high perceptions of privacy risks are associated with a lower intention to use privacy-invasive information systems (e.g., Bélanger and Carter 2008; Xu et al. 2011a; Xu and Gupta 2009) and intentions to disclose personal information in particular (e.g., Li et al. 2014; Xu et al. 2009).

Risk perceptions are thereby measured by asking survey participants to indicate the extent to which they agree to statements like “There would be high potential for loss associated with giving (the information) to online firms” or “Providing online firms with (the information) would involve

many unexpected problems” (Malhotra et al. 2004, p. 352). However, what has remained unconsidered to date is whether survey participants are able to evaluate the risks associated with the disclosure of a certain set of their personal information in the first place. It might well be, that they are simply unable to tell whether disclosing, for example, address information while using a certain privacy-invasive information system is associated with low, mediocre or high privacy risks. This ability or inability to inherently judge the quality of product attributes is discussed in psychology under the term *evaluability* (Hsee et al. 1996; Hsee 2000; Hsee and Zhang 2010). Evaluability is defined as “... the extent to which a person has relevant reference information to gauge the desirability of target values and map them onto evaluation” (Hsee and Zhang 2010, p. 344f.). Thus, if people lack the ability to inherently judge privacy risks, the evaluation of privacy risks becomes dependent on what information is available to survey participants in different contexts. The consequence for IS privacy research would be highly problematic. Measurements of perceived risks of information disclosure would have to be interpreted against the background of how easy to evaluate they were in the study at hand. This would impose vast limitation on the comparability and integrability of existing IS privacy studies.

The reason why privacy risks might be difficult to evaluate is that they are not a simple passive registration of sensory input. They are rather the result of a complex cognitive process, in which external stimuli are selected, organized and interpreted (Solomon et al. 2006). In the case of privacy risk perceptions, relevant stimuli include the requested amount of personal information (Phelps et al. 2000), privacy policies (Gerlach et al. 2015) or privacy seals (Huang et al. 2005). Firstly, these stimuli have to draw an individuals’ attention to become incorporated in the perception formation process. During the following interpretation phase individuals “assign meaning to stimuli” (Solomon et al. 2006, p. 137) by relating them to personal preferences, knowledge acquired through prior experiences or external sources and other perceptions. Relevant preferences in the area of IS privacy research include, for example, one’s individual risk-taking propensity (e.g., Xu et al. 2005) or innovativeness (e.g., Li et al. 2016). Knowledge or perceptions to be considered include, for example, prior experiences of privacy violations (e.g., Bansal et al. 2016; Xu et al. 2011a), the awareness of legislative protection (e.g., Xu et al. 2012), the trust towards an application provider (e.g., Bélanger and Carter 2008; Kesharwani and Bisht 2012) or how relevant the information to be disclosed are for the purpose of the information system (e.g., Sarathy and Li 2007; Sharma and Crossler 2014). Consequently, the formation of privacy risk perceptions is a complex cognitive process based on a great number of external and internal information.

Now the question arises, whether all this information is typically available to individuals when they are asked to indicate their perceived privacy risks. Looking at extant research, it seems that oftentimes it is not (Acquisti et al. 2015; Acquisti and Grossklags 2005b, 2005a; John et al. 2011; Tsai et al. 2011). For instance, it is usually not observable for users when and which information is collected about them (Acquisti et al. 2015) or how their personal information is used by the party it was disclosed to (Acquisti and Grossklags 2005a; 2005b). Furthermore, individuals seem to be unsure about their own privacy-related values and preferences (Acquisti et al. 2015), which could serve as reference information external stimuli can be compared to (Creyer and Ross 1997). The lack of (1) privacy-related knowledge, (2) information about the functioning of privacy-invasive information systems and (3) internal privacy-related preferences leads us to assume that the evaluability of the privacy risks associated with the disclosure of a certain set of personal information is low in general.

What are the consequences of this low evaluability when measuring the perceived risks of information disclosure? Various studies have been conducted, showing that individuals become unresponsive to changes in the value of an objective attribute if its evaluability is low (Hsee 1996b; Hsee 1998; Hsee 2000; Hsee and Zhang 2010). This results from the lack of "... knowledge about which value on the attribute is evaluatively neutral, which value is the best possible, which is the worst possible, what the distribution of the attribute is, and any other information that helps the evaluator map a given value of an attribute onto the evaluation scale" (Hsee et al. 1999, p. 578) described in the prior paragraph. Transferred to information disclosure situations, this implies that if sufficient information is unavailable to study participants, they cannot tell whether disclosing for example address information while using a privacy-invasive information system is associated with low, mediocre or high privacy risks. In such a situation, individuals have the tendency to rate an attribute to be neutral on average (Hsee et al. 1999). The statistically observable relationship between the amount of information gathered by a privacy-invasive information system and the perceived risk of information disclosure it evokes would therefore be insignificant or relatively small in low-evaluability situations.

However, the evaluability of a generally difficult to evaluate attribute can be increased by providing the evaluator with additional reference information (Hsee et al. 1999). An increased evaluability would result in an increased sensitivity to attribute values and therefore also a more pronounced statistical relationship between the amount of personal information gathered by a privacy-invasive information system and the perceived risk of information disclosure. A common and widely used approach of providing such reference information is by letting individuals evaluate products in two different evaluation modes: single and joint evaluation (Bazerman et al. 1999; González-Vallejo and Moran 2001; Hsee 2000; Hsee et al. 1999). Suppose for example two information systems of which one requires users to disclose more information than the other. In single evaluation mode, each of the applications is evaluated by a different group of evaluators who are not aware of the other application. In this case evaluability should be low resulting in low sensitivity towards the amount of information to be disclosed and similar risk perceptions towards both applications. In joint evaluation mode one group of evaluators is confronted with both information systems and rates them simultaneously. In this mode, individuals can compare the amounts of information gathered by both systems. Such a comparison facilitates evaluation as the relationship between the amount of information disclosed and the resulting privacy risks is monotonic (disclosing additional information always alters the privacy risks in the same direction) and individuals know which direction of the attribute is associated with lower/higher risks (the more information being disclosed, the higher the resulting privacy risk). It is therefore obvious that the application requiring more personal information is associated with higher privacy risks in joint evaluation mode. Thus, the amount of personal information gathered by the information systems should exert a greater influence on the perceived risks of information disclosure. Therefore our first two hypotheses as depicted in Figure 8 are the following:

H1: The amount of personal information gathered by an information system is positively related to the perceived risk of information disclosure.

H2: The magnitude of effect of the amount of information gathered by an information system on the perceived risk of information disclosure is greater in joint evaluation mode compared to single evaluation mode.

After elaborating on the formation of perceived privacy risks against the background of evaluability of the amount of information gathered by an information system (RQ1), we now turn

to the effects of perceived privacy risks formed under conditions of easy vs. difficult evaluability (RQ2).

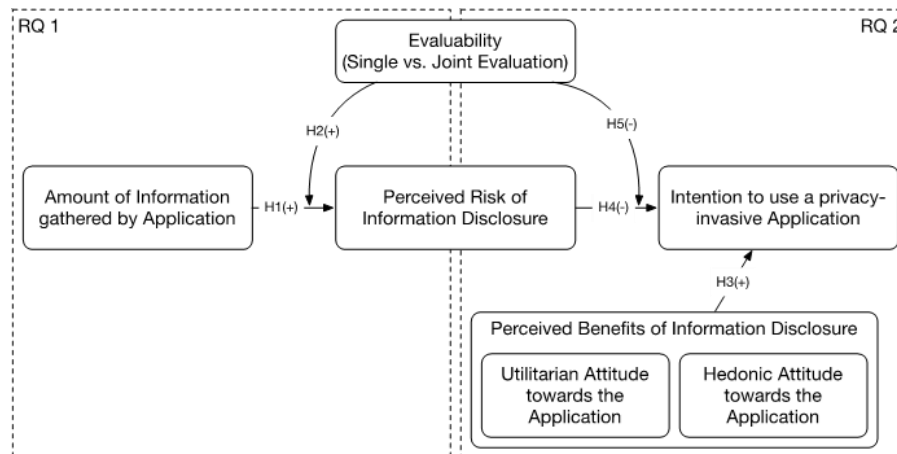


Figure 8. Research model.

The Effects of Risk Perceptions Formed in Different Evaluation Modes on User Behavior

In the previous section, we elaborated on how privacy risk perceptions are formed and thereby differentiated between contexts in which they are easy vs. difficult to evaluate. However, the evaluability of an attribute does not only influence an individual's reaction to objective stimuli and therefore the formation of perceptions, but also how these perceptions influence behavior. This is referred to as evaluability bias: "the tendency to weight the importance of an attribute in proportion to its ease of evaluation" (Caviola et al. 2014, p. 304). Hence, the evaluability of personal information disclosed via a privacy-invasive information system might not only affect the formation of risk perceptions but also the effect of privacy risk perceptions in subsequent decision-making. In the IS privacy context, subsequent decision making based on privacy risk perceptions almost unanimously refers to the decision whether the disclosure of personal information to a privacy-invasive information system is acceptable and therefore whether individuals intend to use a certain privacy-invasive information system (e.g., Bélanger and Carter 2008; Xu and Gupta 2009; Xu et al. 2011a).

This section is therefore concerned with the question how risk perceptions formed under low vs. high evaluability conditions affect individuals' behavioral intentions to use privacy-invasive information systems (RQ2). The theoretical basis of this consideration in IS privacy research is privacy calculus theory (Laufer and Wolfe 1977; Li 2012; Morosan and DeFranco 2015; Wang et al. 2016; Xu et al. 2009), which we adopt as foundation of our research. According to privacy calculus theory, individuals perform a rational tradeoff between the perceived benefits and risks of information disclosure when forming an intention to use a privacy-invasive information system. The corresponding research hypotheses are as follows:

H3: The perceived benefits of information disclosure are positively related to the behavioral intention to use a privacy-invasive information system.

H4: The perceived risks of information disclosure are negatively related to the behavioral intention to use a privacy-invasive information system.

These hypotheses imply, that privacy calculus theory assumes a simple linear relationship between the perceived risks of information disclosure and an individual's behavioral intention to disclose personal information. The higher the perceived risk of information disclosure, the less

likely will an individual use a certain information system. The fact that risk perceptions can be the result of different types of deliberations is ignored here. Suppose that in single evaluation mode (and therefore under low evaluability conditions) individuals rate the risks of information disclosure according to gut feeling. They have a vague idea about how large risks might be, but cannot really reason their perceptions. However, if we measure an individual's perceived risk of information disclosure with established scales like those by Malhotra et al. (2004) or Dinev et al. (2006), individuals will still indicate some amount of risk – maybe even the same amount as a person with all information about the actual risk at hand (and therefore under high evaluability conditions). These two measurements are then indistinguishable with respect to state-of-the-art methods of measuring risk perceptions. Hence, they are regarded to be conceptually equivalent in privacy calculus theory and should exert the same effect on the behavioral intention to use a privacy information system.

Against the background of evaluability theory, this assumption does not hold. Evaluability theory proposes that the two risk ratings described above – albeit being equivalent in terms of their extremity – should differ with regard to their importance in decision making and therefore also behavior formation (Caviola et al. 2014). In particular, a risk perception formed in joint evaluation mode (and therefore high evaluability conditions) should exert greater impact on an individual's behavioral intention to use a privacy-invasive information system compared to a risk perception of equal extremity formed in single evaluation mode (and therefore under low evaluability conditions). This is because evaluability - as a property of a product attribute - is closely linked to the concept of confidence (Boldt et al. 2017), which is a property of a perception evoked by a product attribute (Lichtenstein and Burton 1988). The confidence of a perception is defined as the degree to which an individual has "... a sense that his beliefs and judgements are veridical" (Kelley 1973, p. 107). It resembles in how far individuals were able to use causal inferences to establish the validity of their perceptions. This ability depends on how much consistent information was at hand while forming a perception (Mizerski et al. 1979) and therefore on evaluability. For product attributes with low-evaluability like privacy risks, only few reference information about the quality of the attribute is available to individuals inherently. If this information is missing, confidence in one's own perceived risks of information disclosure should be low. If evaluability is increased by providing additional information, individuals should be more confident that the privacy risks they perceive are valid.

The confidence of a perception resulting from the evaluability of underlying product attributes has been shown to moderate this perception's effect in subsequent decisions (Lichtenstein and Burton 1988). The lower the evaluability of a product attribute and therefore the confidence in a resulting perception, the lesser will this perception influence behavioral reactions. Therefore we extend privacy calculus theory by taking into account, that the magnitude of effect of risk perceptions formed in single evaluation mode (low evaluability and therefore low confidence) should be smaller than that of risk perceptions formed in joint evaluation mode (high evaluability and therefore high confidence). Thus, our last hypothesis is the following:

H5: The effect of the perceived risks of information disclosure on the intention to use a privacy-invasive information system is greater in joint evaluation mode compared to single evaluation mode.

The complete research model with all constructs and hypotheses is depicted in Figure 8.

Research Method

In order to test the formulated hypotheses, we designed a scenario-based experimental survey study, which investigates how different amounts of information gathered by a smartphone app are evaluated in single vs. joint evaluation mode (Hsee et al. 1999) and in how far these risk perceptions influence individuals' usage intentions. Our survey was based on a hypothetical scenario. The use of hypothetical scenarios is a common approach in IS privacy research (Hann et al. 2007; Malhotra et al. 2004; Pan and Zinkhan 2006), because contextual variables have been found to have a strong influence on privacy-related decisions (Smith et al. 2011). Scenario-based surveys allow to maintain a high degree of control over the independent and contextual variables and thereby minimize the effects of disturbance variables (Aviram 2012; Finch 1987; Xu and Teo 2004).

A smartphone application was deliberately chosen as context for our study because of (1) their broad dissemination and the resulting familiarity with this type of applications, (2) the simple adoption process, (3) the structured presentation in smartphone app stores facilitating comparisons and the (4) clear and explicit presentation of information such applications require access to. The number of 149.3 billion smartphone app downloads worldwide in 2016 (Perez 2017) reflects how common it is for humans to search for and to evaluate this kind of applications. The presentation of apps to users is largely defined by the smartphone's app store and therefore similar across all apps. In addition, it is common for smartphone apps to ask users to grant them access to a wide range of personal information like photos, contacts or location services (Olmstead and Atkinson 2010). In contrast to other information systems, these permissions are clearly stated and can be precisely listed within an app description. This clearly delineates the personal information that is disclosed when users decide to adopt an application. All these aspects should make the evaluation process especially easy for users in this context. Hence, if we can observe our hypothesized relationships in this setting, they should also hold in settings where evaluability is lower due to the less structured presentation of information systems.

Two different screenshots showing the app store presentation of two hypothetical task management apps were used as experimental manipulations (see Figure 9). A task management app was chosen for three reasons: (1) it is reasonable to believe that this kind of app requires access to personal information stored on a smartphone, e.g., to be able to assign tasks to contacts or show due dates in a calendar, (2) no major market leader provides a task management app that would serve as an unwanted reference point for participants in our experimental study and (3) a task management app is relatively transparent regarding its functionality and therefore easy to evaluate in terms of the benefits it provides to users. This last point is especially important because our research focus is on the evaluability of privacy risks while keeping the benefits easy to evaluate in single- as well as in joint evaluation mode.

Two app store screenshots (see Figure 9) featuring two apps that differed with regard to the amount of personal information they require users to grant access to were carefully crafted. As both applications are presented side-by-side in joint evaluation mode, we followed the approach by Egelman et al. (2013), and also changed the design of the two app logos, so that the research topic under investigation is not too obvious for study participants. It also prevents the study setting from being too artificial. Two initial sets of permissions were chosen based on common permissions apps require access to on smartphones according to Olmstead and Atkinson (2010). Based on this initial set of permissions, we conducted a qualitative pre-study among 22 potential participants of our experimental survey study to iteratively refine and validate the sets of

permissions, the app description and the logos. This was necessary, because the requested permissions should not be too extreme. As individuals rarely have no knowledge at all about an attribute (Hsee et al. 1999), the number and types of permissions have to fall into a certain range which is not perceived as definitely extremely risky or definitely not risky at all in single evaluation mode. During the qualitative pre-study, students of a German university were shown the app screenshots in a randomized manner. Participants were then asked to assess the apps as if they would have just stumbled upon them in the app store and think aloud while doing so. This allowed us to assess which factors caught participants' attention, what they thought about the amount of information both applications required them to disclose and whether enough information about the functionalities of the app have been provided. After each round of interviews the amounts of information required by both apps, the app description as well as the logos were adjusted until both sets of personal information were neither seen as overly intrusive nor completely risk-free, the two logos, albeit being different, were not interfering with these assessments and participants were able to get an idea of the benefits the app provides. For example, an early set of permissions we approached participants with included access to the phone's microphone. This was nearly unanimously evaluated as being extremely invasive and unacceptable for a task management application and therefore unsuitable for the purpose of our study. The final sets comprised access to contacts and calendar for the less intrusive app (application A) and access to contacts, calendar, location data and photos for the more intrusive application (application B, see Figure 9). It is important to note that all information requested by the less intrusive app (application A) is also gathered by the more intrusive one (application B). Thus, the information collected by the less intrusive app is a strict subset of those information collected by the more invasive one. As a consequence, the more invasive app must (objectively) be at least equally risky compared to the less invasive one. The two final application screenshots used as experimental stimuli are depicted in Figure 9. The experimental materials were translated to English for presentation in this paper. The original materials shown to survey participants were in German language (all participants came from Germany) and colored.

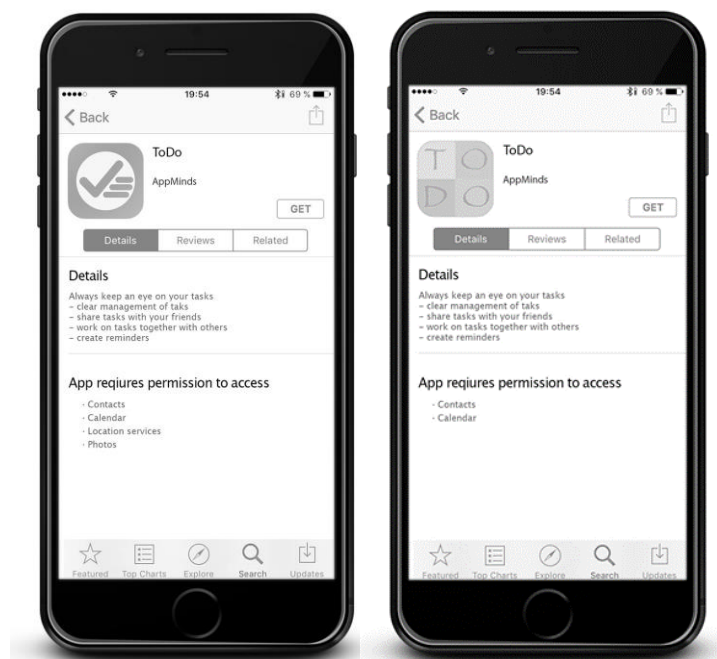


Figure 9. App store screenshots (translated to English), left: application A, right: application B.

The study was carried out as an online survey. Links to the survey were distributed to students of a large German university and via Facebook in February 2017. These channels were chosen because they allow us to reach especially younger participants in the age range between 18 and 34, as these are the largest group of users of mobile apps (comScore 2016). Additionally, younger individuals should have more technology-related knowledge (Margaryan et al. 2011). This knowledge should make it especially easy for them to evaluate the privacy risks associated with a privacy-invasive information system. If privacy risks are even difficult to evaluate for this group, the effect should also hold for less tech-savvy samples. To incentivize the respondents, we raffled gift vouchers.

Participants were first assured that their data would only be analyzed in anonymized form and that there were no right or wrong answers, so they could answer all questions honestly. This was done to counteract common method biases (Podsakoff et al. 2003). After filling out demographic measures (gender, age and employment status), participants were randomly assigned to one of three evaluation modes. Following the study design of Hsee et al. (1999), the evaluation modes are (1) single evaluation of application A, (2) single evaluation of application B, and (3) joint evaluation of both applications side-by-side. Participants were instructed to imagine that they were searching for a task management app in the app store and had just come across the depicted apps. They were then asked to thoroughly investigate them. Participants in the single evaluation modes only rated one app per participant, while those in joint evaluation mode rated both apps. According to Hsee et al. (1999), it is important for participants in the single evaluation mode to only rate one application instead of both sequentially, to make sure that evaluations are made without any reference information. If participants would rate both applications sequentially, the second evaluation could still be influenced by the first one. To make sure this experimental manipulation is successful, a separate study was conducted as suggested by Perdue and Summers (1986). Compared to integrating manipulation checks in the main study, using a separate manipulation check study avoids measures of the dependent variable to bias the manipulation check measures or vice versa (Kidd 1976; Perdue and Summers 1986). While the manipulation check survey used the same three experimental treatments as our main study, it was limited to scales measuring the perceived privacy risks (Malhotra et al. 2004) and a measure of the perceived evaluability of privacy risks. The scale measuring perceived evaluability was self-developed based on the definition of evaluability provided by Hsee and Zhang (2010) and is given in the Appendix 4. Overall, 42 participants took part in the manipulation check survey (21 in single- and 21 in joint evaluation mode). The results show that evaluation modes successfully manipulated evaluability of privacy risks as participants who rated the applications in single evaluation mode perceived the evaluability of privacy risks to be significantly lower ($m = 3.16$) than those who were exposed to both applications in joint evaluation mode ($m = 4.27$, $t = -3.324$, $p = .002$).

In the main study, after being exposed to the application(s), established scales were used to measure all constructs in our research model. To abstract from concrete product features and cover utilitarian as well as hedonic aspects of product benefits, we followed the suggestion of Brakemeier et al. (2016) and operationalized the perceived benefits of information disclosure by the hedonic and utilitarian attitudes towards the apps. These were measured by established scales from Voss et al. (2003). Both scales comprise five semantic differentials like unenjoyable/enjoyable for the hedonic and not effective/effective for the utilitarian dimension of benefits. The perceived risks of information disclosure were measured with the established scale by Malhotra et al. (2004) asking participants to indicate the degree to which they agree to statements like "There would be high potential for loss associated with providing my personal

information to this application.” To measure the participants’ intention to use the app(s), they had to indicate to what extent they would download the application(s) to give it a try by means of four semantic differentials like not probable/probable. This scale was also adopted from Malhotra et al. (2004). Apart from these main constructs, we also measured the participants’ tendency to fantasize (Darrat et al. 2016) as marker variable to test for common method variance (Williams et al. 2010). The tendency towards fantasizing was chosen because it has already been employed as marker variable in a similar context by Son and Kim (2008). Lastly, we adapted a scale by Montoya-Weiss et al. (2003) to measure the visual appeal of the two app logos as a control variable. This variable was incorporated to control for potential influences of the design of the logo on participants’ risk perceptions. All survey items of the constructs in our research model can be found in the Appendix 4.

Apart from making sure all scales used in our survey instrument are established and empirically tested, we also placed emphasis on the fact that our measures comprise a mixture of seven point Likert scales and semantic differentials to prevent common method biases due to common scale formats (Podsakoff et al. 2003). Beyond that, we followed the suggestions of MacKenzie and Podsakoff (2012) and measured the dependent variable before measuring the independent variables and disabled the function to move back to earlier pages of the questionnaire. This was done to prevent participants from changing their answers post hoc to appear rational.

Results

A total of 265 participants completed the survey. To ensure high quality data, we incorporated an instructed response item (Meade and Craig 2012) in our survey. In about the middle of the survey one item was added along the other items measured on a 7-point Likert scale that asked participants to simply check the checkbox most to the right. We used this item to identify participants that did not thoroughly read all items. After eliminating all participants failing at the instructed response item (32), we were left with 233 participants. Of the 233 participants that correctly answered the instructed response item, 103 were assigned to joint evaluation mode and 130 to single evaluation mode (63 application A, 67 application B). To further assure data quality we also investigated the time it took participants to complete the survey. In particular, we checked for downward outliers by computing z-scores for the joint- and evaluation mode samples individually. The largest absolute z-score was 1.61 and therefore well below the threshold of 3 proposed by Kannan et al. (2015). We then conducted another post-hoc check for careless responses as described by Johnson (2005) and Meade and Craig (2012) for the 10% of participants that took the least amount of time to complete the survey. We programmed a visual basic script to compute the Maximum LongString for each participant. This index “... is computed as the maximum number of consecutive items on a single page to which the respondent answered with the same response option.” (Meade and Craig 2012, p. 443). High Maximum LongString values indicate that participants tended to check the same response category for consecutive items and therefore point to inattentive responding. We computed z-scores for the Maximum LongString for each participant and checked for outliers regarding this measure. The largest absolute z-score for participants in single-evaluation mode was 0.83 and for those in joint evaluation mode 0.81. Therefore, no conspicuous participants were found and we proceeded with the responses of all participants that correctly answered the instructed response item. Of those 233 participants, 101 (43.3%) were female. The age of participants ranged from 18 to 64 with the mean being 24.52 ages. The majority were students (79%) or employees (16.3%). As each participant in joint evaluation mode (103) rated both applications, our final dataset comprises a

total of 336 observations in terms of application evaluations of which 130 were made in single evaluation mode and 206 in joint evaluation mode.

We used a structural equation modeling based multi-group-analysis to analyze our data. Structural equation modeling was chosen, because it allows us to test the construct relationships as well as the validity of the measurement model simultaneously (Bagozzi and Yi 1989; Gefen et al. 2000) and thus provides a comprehensive analysis of all relationships in our research model (Fornell and Bookstein 1982). In particular, the variance-based partial least squares multi group analysis as implemented in SmartPLS (Ringle et al. 2015) was employed for two reasons: (1) It is particularly suited to test theories in early stages of development compared to variance-based approaches like LISREL (Fornell and Bookstein 1982) and (2) the multi-group-analysis provided by SmartPLS allows us to simultaneously estimate our research model for the two groups in our experimental study (single vs. joint evaluation) and test whether differences in effect sizes between those models are significant. In PLS multi group analyses, a structural equation model is estimated for two different subsamples. In our case one model is estimated for observations made in joint evaluation mode and one for participants in single evaluation mode. A bootstrapping procedure is then used to assess, whether path coefficients differ significantly between these two models (Hair et al. 2017; Henseler 2012). As we hypothesized that the effect of the amount of data gathered by a privacy-invasive application on the perceived risk of information disclosure as well as the perceived risk of information disclosure on the intention to use the app differ between single and joint evaluation mode (H2 and H5), this method is particularly suited. It allows us to avoid the common practices of noting that an independent variable significantly influences the outcome in one group but not in the other, or that an estimate of magnitude of effect appears to be larger for one group than another, without assessment of the significance of these differences (Brook et al. 1995).

Before analyzing the structural model and testing our hypotheses, we first ensure the validity of the applied measures in our survey for both samples.

Validation of the Measurement Model

The validity of a measurement model is assessed by means of convergent and discriminant validity of the survey instrument (Hair et al. 2014). Convergent validity refers to the degree to which items that were intended to measure the same construct are in fact statistically similar. It is assessed by means of the loadings of items on their constructs, reliability statistics like Cronbach's α and composite reliability (CR) and the average variance extracted (AVE) by the constructs (Xu et al. 2012). According to Hair et al. (2014), item reliability is given when all items have loadings higher than 0.7 on their construct. The item reliability, which is the square of its loading, then is higher than 0.5. This is the case for all items except UTL4, as can be seen in Table 12. However, we decided against omitting the item, because the loadings of 0.676 and 0.698 are only slightly below the threshold of 0.7 proposed by Hair et al. (2014) and well above the threshold of 0.55 suggested by Falk and Miller (1992). The other indicators are given in Table 13. Composite Reliability for all constructs exceeds the threshold value of 0.7 (Bagozzi and Yi 2012; Nunnally 1978) and the average variance extracted is larger than 0.5 for all constructs (Hair et al. 2011). Cronbach's α is also larger than the proposed criterion of 0.7 (Bagozzi and Yi 2012), hence all constructs meet the requirements for convergent validity in the single as well as in the joint evaluation sample.

Table 12. Item loadings and item reliabilities.

Construct	Item	Single Evaluation Mode		Joint Evaluation Mode	
		Item Loading	Item Reliability	Item Loading	Item Reliability
Intention to Use the Application (INT)	INT1	.943	.889	.948	.899
	INT2	.955	.912	.948	.899
	INT3	.944	.891	.940	.884
	INT4	.951	.904	.927	.859
Hedonic Attitude (HED)	HED1	.859	.738	.864	.746
	HED2	.856	.733	.869	.755
	HED3	.875	.766	.908	.824
	HED4	.856	.733	.905	.819
	HED5	.810	.656	.827	.684
Utilitarian Attitude (UTL)	UTL1	.896	.803	.895	.801
	UTL2	.919	.845	.922	.850
	UTL3	.905	.819	.883	.780
	UTL4	.676	.457	.698	.487
	UTL5	.777	.604	.914	.835
Perceived Risk of Information Disclosure (RSK)	RSK1	.849	.721	.886	.785
	RSK2	.805	.648	.909	.826
	RSK3	.924	.854	.922	.850
	RSK4	.792	.627	.867	.752
	RSK5	.717	.514	.716	.513

Table 13. Cronbach's α (Cr. α), Composite Reliability (CR), Average Variance Extracted (AVE) and Construct correlations (single evaluation sample in first lines and joint evaluation sample in second lines).

Construct	Cr. α	CR	AVE	INT	HED	UTL	RSK
Intention to Use the Application (INT)	.963 .957	.973 .969	.899 .885	.948 .941			
Hedonic Attitude (HED)	.906 .924	.929 .942	.725 .766	.620 .259	.825 .875		
Utilitarian Attitude (UTL)	.892 .914	.922 .937	.706 .751	.675 .465	.614 .470	.840 .866	
Perceived Risk of Information Disclosure (RSK)	.877 .912	.911 .936	.673 .745	-.233 -.466	-.123 .096	-.210 -.158	.820 .863

Discriminant validity is given when items intended to measure different constructs are in fact different from other constructs by empirical standards (Hair et al. 2014). For discriminant validity, two conditions have to be met: (1) all items have to load higher on their intended construct than on any other construct (Bagozzi and Yi 2012) and (2) the variance shared between each construct and its items has to be greater than the correlations between the construct and all other constructs (Fornell and Larcker 1981). Although we do not report them in this paper due to space limitations, we investigated all cross-loadings in both samples to assure that they are

substantially lower than the loadings of each item on their respective constructs. As can be seen in Table 13, the variance shared between a construct and its associated items, computed as the square root of the AVE (diagonal elements in Table 13) is greater than all correlations between the construct and any other construct (non-diagonal elements in Table 13) in our model (Fornell and Larcker 1981). Hence, all criteria for discriminant validity are also fulfilled. As a last step, we followed the guidelines by Rönkkö and Ylitalo (2011) to make sure common method variance (Podsakoff et al. 2003) is not an issue with our data and included the tendency to fantasize as a predictor for all endogenous constructs in our model. No regression paths that were significant in the baseline model became insignificant in the model with the marker variable included. Hence, common method variance does not seem to be an issue (Rönkkö and Ylitalo 2011). Descriptive statistics for all variables in our research model can be found in the Appendix 5.

Analysis of the Structural Models

After ensuring our measurement model is valid we proceed by analyzing the overall model quality and the hypothesized construct relationships as reflected by our research model separately for the single evaluation and the joint evaluation sample. Thereby age and gender were incorporated as control variables for the intention to download the application whereas the visual appeal of the logo was used as a control variable for the perceived risks of information disclosure. This was done to control for potential influences of the different logos on the privacy risks evoked by the applications. An issue to be addressed before we proceed with the analysis is the nested structure of our data. In the joint evaluation mode sample, each participant evaluated both apps. We treated these two evaluations as independent observations in the following analysis. This is valid, because “Whereas a covariance-based maximum likelihood (ML) estimation rests on the assumptions of a specific joint multivariate distribution and independence of observations, the PLS approach does not make these hard assumptions” (Chin 2010, p. 659).

The overall model fit as indicated by the standardized root mean square residual are .075 for the joint evaluation sample and .077 for the single evaluation sample. This is below 0.8 and therefore indicating good model fit (Hu and Bentler 1999). Predictive validity of PLS models is assessed by the amount of variance explained in the dependent variables (R^2). Our model explains 39.4% of variance in usage intentions in the joint evaluation sample and 53.3% in the single evaluation sample. R^2 values for the perceived risks of information disclosure are .248 in joint evaluation mode and .02 in single evaluation mode.

Table 14. Results of structural model testing.

	Path Coefficients		p-Values		Multi Group Analysis	
	SE	JE	SE	JE	Difference	p-Value
Application (A=0, B=1) → Perceived Risk	.122 (H1)	.414*** (H1)	.185	.000	.292* (H2)	.031
Perceived Risk → Intention to Use	-.089 (H4)	-.425*** (H4)	.114	.000	.336*** (H5)	.000
Utilitarian Attitude → Intention to Use	.450*** (H3)	.327*** (H3)	.000	.000	.122	.119
Hedonic Attitude → Intention to Use	.332*** (H3)	.158* (H3)	.000	.021	.174	.054

To investigate significance of path estimates, a bootstrapping (Davison and Hinkley 1997) with 5.000 resamples was performed. The path coefficients and their corresponding p-values are reported in Table 14. None of the control variables had a significant influence in either of the models. In particular, the visual appeal of the app's logos was not associated with the perceived risk of information disclosure evoked by the applications. Our first two hypotheses (RQ1) were concerned with the effect of the amount of personal information gathered by an information system on the perceived risk of information disclosure. We found this effect to be significant in joint evaluation mode ($\beta=.414$, $p=.000$). However, the amount of information required by the application did not influence risk perceptions ($\beta=.122$, $p=.185$) in single evaluation mode. Therefore, H1 is only partially supported. The multi group analysis revealed that this difference between path coefficients is significant (difference=.292, $p=.031$), hence supporting H2.

In line with H5, the effect of the perceived risk of information disclosure on the intention to use the applications also differs between joint and single evaluation (difference=.336, $p=.000$). While the effect is significantly negative in joint evaluation mode ($\beta=-.425$, $p=.000$), no effect was found in single evaluation mode ($\beta=-.0989$, $p=.114$). Hence, H4 is only supported for the joint evaluation sample.

The utilitarian dimension of the benefits of information disclosure influences the intention to use the applications equally strong (difference=.122, $p=.119$) in single ($\beta=.450$, $p=.000$) and joint evaluation mode ($\beta=.327$, $p=.000$). The same holds for the hedonic dimension of benefits (SE $\beta=.332$, $p=.000$; JE $\beta=.158$, $p=.021$; difference=.174, $p=.054$) thus supporting H3.

Discussion

In the following, we relate our findings to extant research and discuss the implications for research and practice. The goal of our research was to show that individuals have difficulties evaluating the privacy risk associated with the disclosure of a certain amount of personal information independently (RQ1) and, as a consequence, perceived privacy risks influence behavior differently when they are formed in conditions that facilitate evaluation compared to when they are difficult to evaluate (RQ2).

By integrating an evaluability perspective (Hsee and Zhang 2010) into IS privacy research and providing empirical evidence for our propositions based on an experimental survey study among 233 participants, we extend existing theory in two ways: First, we provide empirical evidence that individuals react more sensitive to the amount of personal information they are required to disclose in order to use a smartphone app in joint evaluation mode compared to single evaluation mode in terms of privacy risks perceptions. In our study, the perceived privacy risks were not even significantly related at all to whether an app only requires disclosure of contacts and calendar information or location data and photos additionally when apps were evaluated independently. Only if the two apps were shown to participants simultaneously allowing them to compare the two sets of permissions, the perceived privacy risks differed significantly between the two applications.

Empirically showing that the effect of the perceived risks of information disclosure formed in single evaluation mode on the intention to use the apps differs from that of risk perceptions formed in joint evaluation mode constitutes our second extension of theory. In our experiment, the intention to use the applications is completely independent of the perceived risk of information disclosure in single evaluation mode. Only in joint evaluation mode we observed a significantly negative effect of the perceived risk of information disclosure on the intention to use

the apps. These findings have several implications for theory and practice, which we will discuss in the following.

Implications for Research

We see three contributions our findings make to IS privacy research. First, we introduce the context-specific evaluability of information disclosures as an important moderator of the extent to which privacy risks are evoked by the disclosure of a certain amount of personal information. This finding is in line with evaluability theory (Hsee 1996b; Hsee and Zhang 2010) and supports the notion that individuals are regularly lacking clear and consistent innate privacy-related preferences (Acquisti et al. 2015). In our study, we used single vs. joint evaluation modes to alter evaluability. Hence, by simply showing two apps side by side, we altered the risk perceptions towards those apps compared to single evaluation mode. Thus, the perceived risk of information disclosure evoked by an information system is not only dependent on properties of this focal system, but also on those of other information systems that serve as reference. We deliberately chose task management apps as context of our study. For this type of app, there is no clear market leader that intuitively comes to one's mind and might therefore serve as reference. However, if risk perceptions towards instant messaging apps are investigated, it might well be that privacy features of, for example, WhatsApp serve as a reference and alter risk perceptions towards other messaging apps. Still, information systems that might serve as a reference do not have to be exogenous. Evaluability of personal information disclosures could also be altered by factors inherent to a study. This would render measurements of perceived privacy risks incomparable across studies. IS privacy researchers should therefore take this effect into account and consciously reflect which external or internal information could serve as reference for privacy risk evaluation and control for those carefully if necessary.

A second theoretical contribution lies in the conception that the perceived risks of information disclosure may not only be characterized by an extremity (the amount of risk indicated by study participants) but also by their confidence. The concept of confidence is discussed in psychology as a property of perceptions referring to "... a belief about the validity of our own thoughts" (Grimaldi et al. 2015). The confidence of a perception is thereby dependent on "... the evidence on which decisions are based" (Boldt et al. 2017). In our experiment, evidence available for perception formation differed between single and joint evaluation mode. It seems, that the increased amount of reference information in joint evaluation mode has led to reduced "evidence variance" and therefore increased confidence in risk perceptions (Meyniel et al. 2015; Yeung and Summerfield 2014). This could explain the stronger influence of risk perceptions on usage intentions in joint evaluation mode as confidence moderates the effect of perceptions in decision processes (Lichtenstein and Burton 1988). Furthermore, this calls for a reconceptualization of perceived privacy risks as comprising the two dimensions of extremity and confidence (Lichtenstein and Burton 1988) and therefore constituting a more complex concept than is assumed in current IS privacy research. Apart from evaluation mode, the degree to which study participants perceive their risk judgments as valid could also depend on other reference information made available to study participants like privacy policies (Gerlach et al. 2015) or privacy seals (Huang et al. 2005). Thus, confidence might be a moderating variable that should be incorporated in research based on privacy calculus theory (Laufer and Wolfe 1977; Li 2012). This leads us to our third contribution.

Demonstrating that the adverse effect of perceived risks of information disclosure on the intention to use a privacy-invasive information system is stronger, the easier those privacy risks were to evaluate, constitutes a third contribution. The idea that the way in which risk perceptions

are formed affects their consequences has not been considered in extant IS privacy research. It challenges the common conception of privacy calculus theory, that individuals perform rational tradeoffs between benefits and risks when forming an intention to use a privacy-invasive information system (Awad and Krishnan 2006). A rational tradeoff would require an individual to weight the perceived risks of information disclosure equally, independent of how they were formed (Hsee 1996b). As we have shown, this assumption cannot be maintained. Our study highlights that the tradeoff between risks and benefits of information disclosure is much more guided by misperceptions and unstable preferences. Individuals are rather insensitive to privacy risk perceptions in low evaluability situations whereas sensitivity increases in high evaluability conditions. Thus, we introduce evaluation mode as a new moderator in the privacy calculus. On a more general level and taking into consideration our second contribution as well as common theoretical reasoning (Lichtenstein and Burton 1988), one could also argue that the confidence in one's own perceived privacy risks moderates their effect on the behavioral intention to use privacy-invasive information systems. Future studies building upon privacy calculus theory should consider the moderating effect of the evaluability of privacy-relevant information system properties in their research models. This could help to explain inconsistencies in previous research based on the privacy calculus. Among these studies, the effects of the perceived risks of information disclosure on behavioral intentions vary widely. While some studies found no effect at all (e.g., Kelley et al. 2013; de Kerviler et al. 2016), others found very strong relationships (e.g., Lee 2009). These dissonant findings could be explained by differences in the evaluability of privacy risks. Furthermore, omitting differences in evaluability could threaten the external validity of privacy calculus studies. External validity denotes the degree to which research results can be transferred to real life settings (Kirk 2014). If evaluability differs between oftentimes artificial situations in privacy studies (e.g., Pan and Zinkhan 2006; Sheng et al. 2008; Son and Kim 2008) and the corresponding real life situations research aims to explain, transferability of research results to real life situations might be impaired.

Implications for Practice

Apart from these theoretical contributions, our findings can also inform users and providers of privacy-invasive information systems as well as policy-makers. Users of privacy-invasive information systems should be aware of their fallibility when assessing the privacy risks associated with the disclosure of a certain amount of personal information to an information system. Privacy risks might be underestimated due to an individual's inability to adequately judge privacy risks independently and therefore users might put their privacy at unreasonable risks. Providers of privacy-invasive information systems could make use of this effect by providing users with information helping them to correctly assess privacy risks and thereby turn privacy-friendliness into a competitive advantage. Malicious providers might, however, also take advantage of lacking evaluability by being vague about how risky their application actually is to profit from the tendency to rate risk as mediocre under low-evaluability conditions. As it is their duty to protect individuals from such malicious market actors, policy-makers should intervene here and stipulate providers to facilitate evaluability. This could for instance be realized by requiring providers to make easy-to-interpret cues accessible that provide users with all information necessary about the actual risk associated with a certain information system. Additionally, app store providers are on duty to offer a consistent design and a standardized way to communicate privacy-invasive properties of applications. One could draw parallels to the political discourse about traffic light labels for food to make it easier for customers to differentiate between healthy and unhealthy food here. Similar indicators could be introduced for privacy-

invasive information systems to promote safer behavior and strengthen privacy-friendliness as a competitive advantage.

Limitations and Future Research Suggestions

Our research is the first to integrate evaluability issues into the privacy calculus and thereby question the ability of humans to comprehensively assess the privacy risks associated with the disclosure of personal information independently. Nevertheless, as is the case with every research, the results of this project are subject to certain limitations. A first limitation lies in the fact that we employed a hypothetical scenario in our experimental survey study. Intentions in such a hypothetical scenario might deviate from those in real-life situations. Nevertheless, employing hypothetical scenarios is a common approach in IS privacy research (e.g., Hann et al. 2007; Malhotra et al. 2004; Pan and Zinkhan 2006; Son and Kim 2008). Furthermore, we deem the approach of employing a hypothetical scenario acceptable for our study, because our goal was not to explain or predict real life adoption behavior of privacy-invasive information systems. However, future research should also investigate the evaluability of privacy risks in real life situations and thereby provide a clearer inspection of the actual implications of our findings in real-life situations.

Another limitation is of methodological nature. Generally, in experimental designs only one factor should be altered between experimental conditions to prove causality. However, we followed the approach of numerous studies on evaluability (Hsee 1996a), information privacy in general (Bansal et al. 2010) and the study of Egelman et al. (2013) in the app-context and did not only manipulate the amount of permissions requested between the two apps in our study but also changed their logos. This was done in order to avoid the research topic under investigation from being too obvious and artificial in joint evaluation mode. It is therefore not possible to unambiguously state that the different risk perceptions were a result of differences in the amounts of permissions requested by the two apps from a purely methodological standpoint. However, based on theoretical arguments (Malheiros et al. 2013), the insignificant effect of the visual appeal of the logos on the perceived risk of information disclosure as well as evidence from our qualitative pre-study, we deem it reasonable to assume that the different logos did not severely confound our findings.

Future studies could investigate in more detail whether specific personal information or certain sets of information are easier to evaluate in terms of privacy risks than others. The sets of personal information required by the two applications in our experiment were deliberately chosen to evoke different perceptions in joint vs. single evaluation mode. Our qualitative pre-study suggests that certain information (e.g., access to the phone's microphone) are perceived as very risky per se. Evaluability might not be an issue in this case. Our results might therefore not be transferrable to arbitrary situations involving the disclosure of personal information.

The composition of our sample constitutes a third limitation. The majority of our sample was composed by students of relatively young age (mean 24.52). We deliberately chose this age group, because apps are intensively used by younger individuals (comScore 2016). Additionally, younger individuals should have more technology-related knowledge (Margaryan et al. 2011), which should make it especially easy for them to evaluate the privacy risks associated with a privacy-invasive information system. We therefore deem our results transferable to less tech-savvy samples. However, the generalizability of our findings is limited by these sample characteristics. Future studies should try to replicate our results with more diverse and larger samples.

A fruitful area for future research might also be to investigate in more detail, which cues or reference information assist individuals in evaluating information disclosure situations. Researchers could for example investigate different ways of presenting apps to users (Kelley et al. 2013) or highlighting privacy-relevant properties of applications (Bal 2014).

Conclusion

Despite the limitations presented above, we were able to offer theoretical arguments and empirical evidence that individuals have difficulties assigning risk judgments to different amounts of data that is requested from them by privacy-invasive information systems. It can therefore occur that individuals do not incorporate their risk perception into the decision whether to use privacy-invasive information systems, because they are unsure in how far their risk judgement is valid. Future research should therefore deliberately control the amount of information available to participants to ensure external validity of IS privacy studies.

We hope these findings make a useful contribution to IS privacy research by challenging the assumption that individuals perform purely rational risk assessment and proposing that they might frequently go with gut feeling when asked to rate privacy risks.

7 Research Paper 2.B: Overconfidence Bias in Privacy-Related Decisions

Title: Too Confident to Care: Investigating Overconfidence in Privacy Decision Making

Authors: Wagner, Amina; Mesbah, Neda

Published in: European Conference on Information Systems (ECIS), Stockholm, Sweden 2019

Abstract

Labeled as the privacy calculus model, research assumes that individuals perform a rational tradeoff between benefits and privacy risks. However, growing evidence indicates that due to incomplete information and bounded rationality, individuals' decision making is biased. De-rived from behavioral economics literature, overconfidence is one of the most critical bias in decision-making and has drawn little attention in privacy research. Based on an empirical online study among 239 smartphone users, we (1) measure actual privacy knowledge with the help of a quiz and thus provide evidence that overconfidence with regard to privacy exists, as well as (2) show that overconfidence moderates the link between privacy risks and the behavioral intention to use a smartphone application. Additionally, (3) we found the presence of the Dunning-Kruger-effect in our sample with less competent individuals being more overconfident than high performers. Overall, by building on the behavioral economics literature and incorporating a cognitive bias into the privacy calculus model, we extend the privacy calculus and give insights on ambiguous decision making in the context of personal data disclosure. Practical and theoretical implications are discussed.

Keywords: Privacy Calculus, Privacy Risks, Behavioral Economics, Overconfidence, Cognitive Bias.

Introduction

Labeled as the privacy calculus, information systems (IS) research assumes that individuals perform a rational tradeoff between benefits and privacy risks derived from an intrinsic need to maximize their net utility (benefits minus costs) (Culnan and Armstrong 1999; Dinev and Hart 2006). At the same time, information system users are mostly uncertain of how and when their personal information is used (Acquisti and Grossklags 2005b, 2005a), making it difficult to make sound decisions regarding their privacy. Additionally, privacy thefts are commonplace with outcries over privacy caused by the Facebook-Cambridge Analytica scandal (New York Times 2018) and Yahoo (CNBC 2018), among others. Against this background, the question arises: Are individuals able to make well informed and rational privacy decisions?

Indeed, recent evidence building on the behavioral economics literature has shown that privacy risks judgements are subject to cognitive biases demonstrating that users are trapped by their own optimism (Baek et al. 2014; Cho et al. 2010), mental states (Kehr et al. 2015; Brakemeier et al. 2016) or inability to evaluate privacy risks accurately (Brakemeier et al. 2017). Based on this stream of research, users are unable to fully assess privacy risks due to incomplete information, bounded rationality and unstable preferences. Additionally, Acquisti and Grossklags (2005a) have provided preliminary indications that individuals are overconfident with regard to their privacy. 73.1 percent of their survey participants underestimated the probability of becoming an identity theft victim when comparing it to the actual number in the US.

Although, overconfidence is supposed to be the most crucial bias in decision-making (De Bondt and Thaler 1995) deemed to be accountable for stock-market failures (Glaser and Weber 2007) and bankruptcy (Busenitz 1999), to the best of our knowledge, no research to date has investigated overconfidence and its influence on subsequent privacy decisions. Overconfidence is referred to as individual's tendency to overestimate their knowledge or abilities in relation to their actual rate (Oskamp 1965; Russo and Schoemaker 1992). Assuming that individuals are overconfident with regard to their perceived privacy risks, this confounds with the rational tradeoff between benefits and risks typically presumed in extant privacy research (Dinev and Hart 2006; Krasnova et al. 2010a). Thus, we hypothesize based on behavioral economics literature that overconfidence lowers the impact of privacy risks on intention to disclose information as individuals believe they are in control of their privacy. Individuals who overestimate their knowledge and thus their competences do not consider their own risks appropriately. As a result, their personal data disclosure may be less rational compared to those being not overconfident with regard to their competence prediction.

We investigate this theoretical conceptualization based on an online survey among 239 smartphone users. Guided by the research questions: *(1) Do individuals suffer from overconfidence with regard to their privacy?* and *(2) Do perceived privacy risks influence behavior differently when individuals are overconfident?*, we respond to a call from to investigate behavioral biases and their impact on privacy decisions. Furthermore, we explore group differences between overconfident and non-overconfident respondents.

This study's main goals are to uncover overconfidence in privacy knowledge based on a privacy quiz and explore its impact on subsequent decision-making in the context of the privacy calculus. We contribute to theory and practice in several ways. First, based on a privacy quiz we measure actual privacy knowledge and relate it to participants' self-assessed score in order to measure overconfidence. In this vein, we provide evidence of individuals' overconfidence with regard to privacy knowledge and thereby show that overconfidence negatively moderates the link between

privacy risks and personal data disclosure intentions. It challenges the common assumption in privacy research that individuals make rational privacy decisions (Awad and Krishnan 2006). Second, we give a possible explanation why effect sizes of privacy risks on disclosure intentions are controversial between prior studies (e.g., Xu et al. 2009; Kehr et al. 2015; Shibchurn and Yan 2015) by indicating that some study participants are subject to their own error of judgement.

Beyond theoretical implications, our study gives reasons to law makers and organizations that users need privacy training to effectively judge their knowledge and in turn their competence to make sound privacy decisions. This can help users to take care of their privacy whereas privacy-friendly information systems providers can use this awareness to build on privacy as a competitive advantage.

Distortions in Privacy Decision Making

Privacy Calculus and Behavioral Biases

To enrich our motivation and build a theoretical foundation, we first outline literature on the privacy calculus and explain overconfidence as well as its criticality in individuals' decision making.

In today's digitized world where personal information is exchanged for the means of transacting with one another, disclosure decisions have been drawn much research attention. In order to account for individuals' personal data disclosure decisions, IS literature has commonly relied on the privacy calculus (Dinev and Hart 2006; Laufer and Wolfe 1977). Generally, it assumes that disclosure decisions are a result of a rational tradeoff between benefits and privacy risks (Culnan and Armstrong 1999). Stemming from the social exchange theory it is centered on the concept of utility maximization with the underlying goal to maximize benefits and minimize losses (Homans 1958; Laufer and Wolfe 1977). When benefits are perceived as higher than expected privacy risks, individuals are supposed to transact with a provider by giving up their privacy (Culnan and Armstrong 1999). Thereby, individuals are assumed to act as rational agents having all necessary information, being able to calculate parameters and thus make well informed decisions (Tsai et al. 2011).

Despite this assumption, research building on the privacy calculus perspective is not consistent. While some studies have shown that perceived privacy risks are the most influential antecedent for disclosure decisions (e.g., Kehr et al. 2015), others have provided empirical evidence that perceived privacy risks have only a minor effect (e.g., Shibchurn and Yan 2015; Xu et al. 2009) or even no significant effect at all (Krasnova 2012; Wagner et al. 2018c). Moreover, users seem to be reluctant to protect their privacy accordingly (e.g., Norberg et al. 2007) such as on Facebook or other privacy-invasive information systems. Sometimes it even appears as if they give away their personal information for a tiniest benefit (Acquisti et al. 2009). This indicates that there must be interference factors which distort individuals' decision making. In order to account for these distortions in individuals' privacy decision-making, research has started to investigate individuals' decision process from a behavioral economics perspective (Acquisti 2004; Brakemeier et al. 2017).

Behavioral economics literature (among others Kahneman et al. 1982) and its underlying assumption that users do not make well informed decisions have found attention in the privacy context by studies from Acquisti and colleagues (e.g., Acquisti and Grossklags 2005a, 2005b). Immediate gratification (Acquisti 2004) and being endowed with privacy (Acquisti et al. 2009) have been uncovered as psychological interference factors. Inspired by these attempts, research

has shown that situational and dispositional factors like mental states (Brakemeier et al. 2016a), external reference information (Brakemeier et al. 2017; Tsai et al. 2011), affect as well as trust drive ambiguous behavior (Kehr et al. 2015). Furthermore, research has found that individuals are too optimistic about their privacy theft probability when comparing it to averaged others (Cho et al. 2010) or comparison targets (Baek et al. 2014). They perceive themselves at lower risks and a higher level of control referred to as comparative optimism (Weinstein 1980). To conclude, IS privacy literature has started to identify a number of decisional biases (Kahneman et al. 1982) which distort sound self-disclosure decisions.

Overconfidence

Although overconfidence is claimed to be the most crucial bias in humans' decision-making (De Bondt and Thaler 1995), less attention has been drawn to this cognitive distortion in individuals' privacy decision making (for review see Kokolakis 2017). In IS research, overconfidence has been investigated in the context of IT professionals (Vetter et al. 2011) and security in general (Ament 2017) as well as phishing mail detection in particular (J. Wang et al. 2016). On the privacy front, Jensen et al. (2005) and Acquisti and Grossklags (2005a) have indicated that overconfidence is salient, but its impact on subsequent privacy decision making remained untouched. Therefore, we move beyond current research insights and investigate overconfidence in privacy decision-making with a profound approach.

Overconfidence describes individuals' tendency to overrate self-perceived competence in comparison to their actual competence (Russo and Schoemaker 1992). Specifically, it is the extent to overestimate ability, control and success chances (Moore and Healy 2008). Thus, it has also been linked to individuals' illusion of control (Vetter et al. 2011; Chen and Koufaris 2015) referred to "[...] as an expectancy of a personal success probability inappropriately higher than the objective probability would warrant" (Langer et al. 1975, p. 311). It is an extreme form of confidence which is not justifiable against the background of objective performance. Among others, perceived self-efficacy (Moores and Chang 2009), task complexity, and level of motivation (Russo and Schoemaker 1992) have been made accountable to leverage overconfidence.

Overconfidence is primarily present in uncertain situations with unknown probabilities (Russo and Schoemaker 1992) and privacy decision making is subject to a number of uncertainties (Acquisti and Grossklags 2005b): First, whereas benefits are easy to assess (Acquisti 2004) privacy risks are difficult to evaluate (Brakemeier et al. 2017). Individuals are mostly uncertain of how and when their data will be used (Acquisti and Grossklags, 2005b, 2005a). Users might have disclosed it to one information system provider for personalization purposes, but the very same information might be used to target advertisement or to share it with third parties. In this vein, individuals lack complete information to make well informed decisions (Acquisti and Grossklags 2005b). Second, when being confronted with a decision against the background of incomplete information, individuals have to rely on available external information like privacy seals (Tsai et al., 2011) or their own knowledge and perceptions (Hogg et al., 2006). When external information is missing, people commonly utilize their own subjective knowledge as an anchor (Russo and Schoemaker 1992). Previous research on the effects of perceived knowledge has indicated that individuals who believe they are knowledgeable base their decisions on their self-assessed knowledge without requesting consult which results in a high illusion of control and in turn overconfidence (Chen and Koufaris 2015; Gino et al. 2011). Eventually, even when knowledge is objectively high, individuals can overrate their competence and thus expert knowledge alone does not necessarily result in a sound decision (McKenzie et al. 2008). Based on

these results, we presume that overconfidence might be present in privacy decision making due to its uncertain nature.

On the other hand, there is growing research evidence arguing that privacy decisions are a complex task which overwhelms individuals and requires tremendous cognitive resources (Korff and Böhme 2014). For example, in a study of the Pew Research Center Americans state that “I do not have the time or expertise” to enhance privacy (Smith 2014). Furthermore, data breaches have increased during the last years (Statista 2018a) which in turn led to high media presence and awareness of its risks for internet users. Thus, individuals might be more sensitive to their own theft probability and are aware of their knowledge limitation which might lead to a lower probability of overconfidence in privacy decision-making.

Overall, the evidence on the presence of overconfidence in privacy decision making remains controversial. Considering the uncertain and complex nature of privacy decisions, it is unclear whether individuals are subject to overconfidence when disclosing information online. For instance, Acquisti and Grossklags (2005a) showed based on a US sample that privacy knowledge is fuzzy and that risk propensities are either over- or underestimated. Against this background, we investigate the extent of overconfidence in the privacy domain and whether it distorts sound privacy decision-making.

Hypotheses Development and Research Model

In the previous section, we outlined the typically assumed privacy calculus and its underlying rational decision process. Against this background, we provided arguments why individuals’ overconfidence in their privacy knowledge is essential in order to uncover reasons for individuals’ ambiguous privacy decisions. We now build on this theoretical foundation and develop our hypotheses as well as conceptualize our research model, depicted in Figure 10 below.

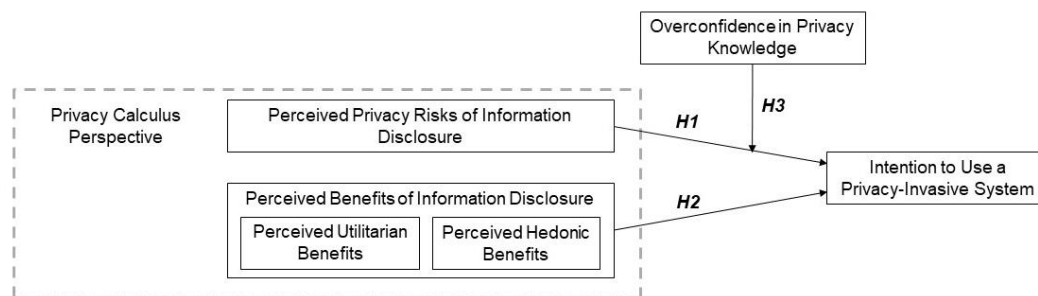


Figure 10. Conceptual research model.

Privacy Calculus

IS privacy research building on the privacy calculus model is concerned with antecedents of individuals’ disclosure decisions when transacting with a privacy-invasive system provider (e.g., Dinev and Hart 2006; Xu et al. 2009). This provider can be any information system that collects, stores and processes personal information about its users (Brakemeier et al. 2017). Since users are mostly uncertain of how and when their personal information will be used, a high level of uncertainty about organizational information practices arises (Acquisti and Grossklags 2005a). Providers can use this information in an unpredictable manner or even share it with third parties (e.g., data-brokers or cooperating firms), which is associated with a worry about organizational information practices (Malhotra et al. 2004). This potential worry is referred to as individuals’ perceived extent of loss of control over their personal data (Smith et al., 2011). It is subsumed under the term “perceived risks of information disclosure” and has been largely investigated as

an impediment of transacting with an provider in general (e.g., Bélanger and Carter 2008; Xu et al. 2011a) and disclosure intentions in particular (e.g., Krasnova et al. 2010a). Therefore, high perceived privacy risks have predominantly been linked to a lower intention (e.g., Krasnova et al. 2010a; Xu et al. 2011a). In line with the privacy calculus perspective, we hypothesize the following:

H1: The perceived privacy risks of information disclosure are negatively related to the behavioral intention to use personal information to a privacy-invasive information system provider.

As privacy risks are weighted against benefits in the course of the privacy calculus, benefits are supposed to drive individuals' intention to disclose personal information (e.g., Kehr et al. 2015; Krasnova et al. 2010a). They form the incentive which is provided to users in exchange for personal information. Those are perceived differently by each individual and highly context-specific. Among others, personalization (Chelappa and Sin 2005), usefulness and social benefits (Krasnova et al. 2010a) have been linked to disclosure decision in previous studies. Therefore, we transfer a two-folded conceptualization of benefits from marketing literature which has recently been introduced to privacy research (Brakemeier et al. 2016, 2017): hedonic and utilitarian benefits (Voss et al. 2003). Utilitarian benefits are stemming from the usefulness and practicability of a service. It describes the extent to which the system helps to fulfill a task. Hedonic benefits go beyond the core features of a system by covering its entertaining features such as enjoyment. By following the privacy calculus, we hypothesize that:

H2a: The perceived utilitarian benefits of information disclosure are positively related to the behavioral intention to use personal information to a privacy-invasive information system provider.

H2b: The perceived hedonic benefits of information disclosure are positively related to the behavioral intention to use personal information to a privacy-invasive information system provider.

Extension of the Privacy Calculus

Building on the privacy calculus model (Culnan and Armstrong 1999; Dinev and Hart 2006), prior IS literature has consistently assumed a linear relationship between benefits and risks with behavioral intentions (Li 2012). However, in line with the behavioral economics perspective (Kahneman et al. 1982), we now develop our hypotheses which extends the privacy calculus and challenges its assumption of being a rational balancing act.

Against the background of behavioral economics, perceived knowledge can be subject to overconfidence (McKenzie et al. 2008). It is a false perception of being in control of uncertain events (Chen and Koufaris 2015; Vetter et al. 2011). Simply spoken, individuals think that they can deal with the perceived risk and thus care less about it (Ament and Jaeger 2017). Building on this conceptualization, overconfidence of a perception has been shown to moderate this perceptions' effect in subsequent behavioral decisions (e.g., Moores and Chang 2009). For instance, entrepreneurs are usually overconfident about their skills even though they are aware of the potential risk to not succeed in the marketplace (Busenitz 1999). Additionally, notorious speed merchants are usually aware of their severe accident risk but continue to drive fast because they believe that they are in control of future events (Weinstein 1980). Transferred to the privacy domain, when individuals believe they are in control with regard to their own information privacy, they are positively framed regarding their privacy risks which in turn leads them to be less overwhelmed by the extremity of that risk and behave more tolerant towards it (Heath and

Tversky 1991). As such, some individuals who falsely believe in their competence take more risky options while being less focused on risks (Krueger and Dickson, 1994) whereas non-overconfident individuals are more aware of their fallibility. If confidence in ones' own privacy competence is low, individuals are uncertain of their own abilities to handle the risk and thus individuals should be more focused on their perceived risk extremity. They are negatively framed with regard to their own privacy competence and in turn risk perceptions play a role in their behavioral decision making.

As a result, we cannot assume a linear relationship between privacy risk judgements and information disclosure intentions. This relationship is dependent on individuals' anticipation of their own competence in this field. Specifically, when individuals are overconfident, the less will individuals take their own perceived privacy risks into account as they are less focused on risks. Benefits in contrast are more easy to evaluate and thus they are less likely to be subject of misperceptions (Brakemeier et al. 2017). Therefore, we extend the privacy calculus by presuming that overconfidence in ones' privacy knowledge moderates the link between privacy risks and intention to use whereas individuals who are non-overconfident consider their own risk perceptions accordingly. Thus, we hypothesize the following:

H3: The effect of the perceived risks of information disclosure on the intention to use a privacy-invasive information system is lower for users who are overconfident compared to users who are not overconfident about their privacy knowledge.

Method

In order to measure our conceptual model, we conducted a quantitative online survey which measured (1) individuals' overconfidence based on a privacy quiz and (2) to what extent this overconfidence influences usage decisions. We relied on a hypothetical scenario which is a common approach in privacy research (Malhotra et al. 2004; Hann et al. 2007; Son and Kim 2008), because of the context-sensitive nature of privacy decisions (Smith et al. 2011).

We decided to frame our study to the context of smartphone applications for three main reasons. First, it is a widely used context which was found to be applicable for privacy decisions (e.g., Keith et al. 2015; Xu et al. 2009). Second, smartphone apps are nowadays used on a daily basis (Statista, 2016) and thus the decision to use an app should be common among study participants. Third, smartphone apps are supposed to be privacy-invasive as they request access to personal information like contact details, location data and calendar information (Olmstead and Atkinson, 2015). Furthermore, there is a clear and explicit presentation of the information requested and most of the time the presentation is defined by the smartphone's app store so that the presentation of an app is similar across all apps. We followed the assumptions by Brakemeier et al. (2017) and relied on a "ToDo" app as its functionalities are easy to understand. Our fictional app requests permission to four types of personal information (contacts, calendar, location, photos). Against the background of an examination of Google Play Store Apps by the Pew Research Center, this type and the number of requests are typical (Olmstead and Atkinson, 2015) and also justifiable for a ToDo app.

The participants were acquired with the help of a market research firm. A market research firm offers the benefit of targeting an anonymous and diverse population of internet users regarding their age, gender and employment status (for justification see Lowry et al. 2016). By doing so, we asked for smartphone users aged between 18 and 66 years. The survey commenced with a welcome page where participants were informed that participation in the survey is anonymous

and that there are neither right nor wrong answers. This reference is made to counteract common method biases (Podsakoff et al. 2003). On the next page, participants were instructed to imagine that they are looking for a ToDo app and have just come across our (fictional) app in the app store. A graphical illustration (screenshot) of the app with a short description of its main functionalities was presented to the participants. Afterwards, individuals were presented with the survey items representing the main constructs of the research model followed by the privacy quiz as a last step.

All of our construct measurements have been taken from established literature and can be found in Table 15. Perceived privacy risks have been measured with five items from Malhotra et al. (2004) based on a 7-point Likert scale ranging from 'strongly disagree' to 'strongly agree'. All other main constructs were measured on a 7-point semantic differential. To measure perceived benefits of information disclosure, we relied on a global scale from Voss et al. (2003) and operationalized the perceived benefits of information disclosure by the hedonic and utilitarian attitudes towards the apps. To evaluate the participant's intention to use the apps, we adopted a scale from Malhotra et al. (2004). To counteract common method bias (Podsakoff et al. 2003), we also included the tendency towards fantasizing as a marker variable which was tested to be suitable in the privacy context (Son and Kim 2008). It was measured on a 7-point Likert scale ranging from 'strongly disagree' to 'strongly agree' with three items lend from Darrat et al. (2016): "I daydream a lot", "When I go to the movies, I find it easy to lose myself in the film" and "I often think of what might have been".

Beyond sociodemographic data, we also included several control variables applicable to our context. Previous privacy experience was taken as respondents might be more sensitive to privacy-invasive information systems like apps when they were past victims of a loss of privacy. Thereby, we relied on the scale of Xu et al. (2009) comprising two items measured on a 7-point Likert scale ranging from 'never' to 'very often': (1) "How often have you personally been victim of what you felt was an invasion of privacy?" and (2) "How much have you heard or read during the last year about the use and potential misuse of computerized information about consumers?". Likewise Ament (2017), we measured the perceived difficulty level of the privacy quiz for oneself and for an average internet user on a 7-point Likert scale ranging from 'not at all difficult' to 'very difficult'.

In order to measure respondents' privacy knowledge, we developed an objective privacy test with 10 multiple-choice answers as recommended by Russo and Schoemaker (1992). This approach was validated by Aggarwal et al. (2015) who tested actual and perceived IT-knowledge of employees and Ament (2017) who tested actual and perceived information security knowledge of subjects. By building on this approach, we were able to capture actual privacy knowledge. Privacy knowledge in particular, describes the extent to which individuals' are informed about organizational information practices (Naresh K. Malhotra, Sung, et al. 2004), privacy regulations (Pu and Grossklags 2016) and countermeasures (Culnan 1995). The 10 multiple-choice questions were developed as follows: We first reviewed literature on privacy knowledge which yield two privacy knowledge tests (Park and Jang 2014; Trepte et al. 2015). The one from Park and Jang (2014) measures individuals' knowledge in the mobile context with seven questions while the one from Trepte et al. (2015) is seeking to comprehensively capture privacy knowledge with a 20-item scale including law and technology related questions. Based on these two scales and expert discussions, we invented a 22-item long questionnaire catalogue. We pretested this quiz with 42 participants (mean age: 28.9; 59.5% females), recruited via an email panel list. We thereby assessed, the difficulty, the required time and the comprehensiveness of the questions. After an iterative process with four academic privacy experts, our test comprised 10 multiple-choice

questions with two response options (false, true) which can be found in Appendix 6. Since many questions are related to the extent to which information system providers store and process personal information and its underlying law regulations, the privacy quiz fits adequately to our smartphone context.

Despite respondents' actual privacy knowledge based on the test score, we were also interested in their perceived privacy knowledge. Participants had to estimate their actual score after taking the test: "What do you think, how many of the 10 questions did you answer correctly?" (Aggarwal et al. 2015). Thereby, we were able to calculate the presence of overconfidence by subtracting the self-reported amount of correctly answered questions from the actual amount as recommended by Moore and Healy (2008). This specific equation is termed overestimation in Moore and Healy (2008) and is commonly used as a proxy for overconfidence (e.g., Malmendier and Tate 2005). In line with Moores and Chang (2009), this helped us to categorize our participants in overconfident and non-overconfident as a binary group variable. When being fully accurate about their test scoring, meaning that their actual score is commensurate with their expected score, or at least the difference is greater than zero, they were assigned to the group of non-overconfident individuals. In contrast, where the difference is below zero, i.e. expected score is higher than the actual score, they were categorized as being overconfident. Except of overestimation as a measure of overconfidence, there are a number of other potential equations (Moore and Healy 2008). We decided to rely on overestimation as it is the most stable form of overconfidence (Russo and Schoemaker 1992) and it captures purely individuals' overconfidence without interference of other related biases such as comparative optimism (Hilton et al. 2011).

Results

Overall, 261 respondents took part in our survey. To eliminate participants who were not seriously involved in the survey, we included an attention check (Meade and Craig 2012) into our survey. 22 participants failed the attention check and thus we were left with 239 participants for further analyzes. Of those, 48.5% were females and the remaining 51.5% were males. The samples mean age was 36.09, ranging from 18 to 60 and most of them were employees (54.8%) followed by students (25.1%). Thus, our samples' age, gender and employment status is almost equally distributed to European internet users (Eurostat 2018). The participants perceived our test as moderately difficult (mean = 3.71). Of the 239 participants, 41 were overconfident and 198 were not overconfident.

We used structural equation modeling as implemented in SmartPLS to analyze our data (Qureshi and Compeau 2009). For evaluation of the group differences and thus the moderation of overconfidence, we used the variance-based partial least squares multi group analysis (Ringle et al. 2015). This approach is convenient to test theories in early stages of development (Fornell and Bookstein 1982). Furthermore, the multi-group-analysis provided by SmartPLS enables to test our research model for the two groups as well as the significant differences in path coefficients in parallel (Brook et al. 1995). This method is robust to group-specific parameters, i.e. it is able to handle group size differences (Sarstedt et al. 2011). According to the 10 times rule, the minimum group size should be ten times of the maximum number of arrows conceptually related to a latent variable (Hair et al. 2013). This criteria is fulfilled in our data set with both groups comprising more than 30 observations.

Validation of the Measurement Model

Before proceeding with the analysis of the construct relationships and thus testing our hypotheses, we first ensure the validity of our measurement model by means of convergent and discriminant validity of the research model (Hair et al. 2013). To start with convergent validity, it describes the degree to which items which measure the same construct are in fact statistically similar. It is tested by the items reliability as well as by reliability statistics like Cronbach's α and composite reliability (CR) and the average variance extracted (AVE) by the constructs (Xu et al. 2012). Assessing item reliability of our measurement model, we report the factor loadings of the items with their intended construct in Table 16. As all items have loadings higher than 0.65, our items are of sufficient reliability (Falk and Miller 1992). Depicted in Table 17, Cronbach's α and composite reliability were above the required threshold of 0.7 (Hair et al. 2013) and AVE was above 0.5 (Hair et al. 2011) for all constructs.

To test for discriminant validity, we examined the square root of the AVE for each construct and ensured that it was higher than the correlation between this and any other construct in the model (Fornell and Larcker 1981). All items loaded highest on their anticipated factor (see Table 17 on the next page). Cross-loadings were not an issue. All in all, the measurement models demonstrate reliability and validity.

Table 15. Survey items and item loadings (OC=overconfident; NOC=non-overconfident).

Constructs (measured on 7-point scales)	Items		Item Loadings	
			OC	NOC
Intention to Use the Application (INT)	INT1	Unlikely / Likely	.858	.945
	INT2	Not probable / Probable	.966	.959
	INT3	Impossible / Possible	.957	.952
	INT4	Unwilling / Willing	.956	.943
Hedonic Attitude (HED)	HED1	Not fun / Fun	.910	.913
	HED2	Dull / Exciting	.933	.917
	HED3	Not delightful / Delightful	.864	.887
	HED4	Not thrilling / Thrilling	.831	.837
	HED5	Unenjoyable / Enjoyable	.877	.853
Utilitarian Attitude (UTL)	UTL1	Ineffective / Effective	.932	.902
	UTL2	Unhelpful / Helpful	.951	.930
	UTL3	Not functional / Functional	.949	.889
	UTL4	Unnecessary / Necessary	.953	.946
	UTL5	Impractical / Practical	.959	.930
Perceived Risk of Information Disclosure (RSK)	RSK1	In general, it would be risky to disclose my personal information to this application.	.892	.892
	RSK2	There would be high potential for loss associated with providing my personal information to this application.	.907	.866
	RSK3	There would be too much uncertainty associated with having my personal information gathered by this application.	.935	.927

	RSK4	Providing the provider of the application with my personal information would involve many unexpected problems.	.841	.820
	RSK5	I would feel safe giving my personal information to the provider of this application. (reverse)	.684	.771

Finally, we assessed the existence of common method variance (Podsakoff et al. 2003) in our data. Therefore, we followed the guidelines by Rönkkö and Ylitalo (2011) and included our marker variable as a predictor for all independent variables in our model. This variable does not change the significance of relationships in our baseline model and thus we believe that it is unlikely that common method bias is an issue.

Table 16. Cronbach's α (Cr. α), Composite Reliability (CR), Average Variance Extracted (AVE) and Construct correlations (overconfident in the first and non-overconfident in the second row).

Construct	Cr. α	CR	AVE	INT	HED	UTL	RSK
Intention to Use the Application (INT)	.952 .964	.965 .974	.875 .902	.935 .950			
Hedonic Attitude (HED)	.930 .929	.947 .946	.781 .778	.790 .644	.884 .882		
Utilitarian Attitude (UTL)	.972 .954	.978 .965	.900 .846	.721 .624	.700 .738	.949 .920	
Perceived Risk of Information Disclosure (RSK)	.908 .908	.932 .932	.734 .734	-.183 -.606	.030 -.357	-.221 -.388	.857 .857

Analysis of the Conceptual Model

After testing that the measurement models demonstrate reliability and validity, we initially analyzed the relationships in our model without taking into account 'overconfidence'. We thus present the results for the full sample model derived from bootstrapping with 5,000 re-samples (Davison and Hinkley 1997). All path coefficients and significance levels were in line with H1 and H2a/b and thus as assumed in the established privacy calculus model. Perceived risk of information disclosure is negatively related to intention ($\beta = -.340$, $p = .000$) and thus supports H1. A positive relationship between perceived utilitarian benefits ($\beta = .217$, $p = .004$) and hedonic benefits ($\beta = .413$, $p = .000$) with intention to use were found to be significant, thus supporting H2a and b.

Proceeding with the influence of overconfidence within the privacy calculus, the model fit is .067 for the overconfident sample and for the non-overconfident sample .057. This is indicating a good model fit as it is below the cut-off criteria of 0.08 (Hu and Bentler 1999). Our model explains 69.8% of variance in usage intentions in the overconfidence sample and 59.8% in the non-overconfident sample. In the next step, we tested the moderation effect of overconfidence by computing a multi-group-analysis. The significance of the path coefficients is reported in Table 17. Even though risk perceptions do not significantly differ between both groups (independent-samples t-test: $t = 1.311$; $p = .191$), its effect on the intention to use the application differentiates, as postulated in H3.

Perceived risk has a significantly negative effect on intention to use for the non-overconfident sample, but no significant effect could be found for the overconfident sample. Hence, H1 is only supported for the non-overconfident samples and thus perceived privacy risks of information disclosure are differently perceived by both groups. Utilitarian and hedonic dimensions of the benefits of information disclosure do not influence the intention to use the application differently

in two groups. However, the utilitarian dimension of the benefits are not significantly linked to the intention to use for the overconfident sample, whereas it has a significantly positive effect for the non-overconfident group. Hence, H2b is supported for both samples and H2a is only supported for the non-overconfident sample.

Table 17. Effect sizes and results of structural model testing (** $p < 0.001$; ** $p < 0.01$; * $p < 0.05$).

	f^2		Path Coefficients		p-Values		Multi Group Analysis	
	OC	NOC	OC	NOC	OC	NOC	Difference	p-Value
Perceived Risk → Intention to Use	.060	.334	-.143 (H1)	-.400*** (H1)	.210	.000	.257* (H3)	.017
Utilitarian Attitude → Intention to Use	.102	.051	.261 (H2)	.217** (H2)	.207	.002	.045	.488
Hedonic Attitude → Intention to Use	.589	.130	.612** (H2)	.341*** (H2)	.005	.000	.270	.159

Finally, we analyzed whether there are significant group mean differences with regard to age (in years), privacy experience and actual privacy knowledge (amount of correct answers within the privacy quiz) by running independent t-tests, depicted in Table 18. Despite of actual privacy knowledge, none of them turned out to be significantly different between the two groups. The effect size of actual privacy knowledge ($g^{\text{Hedges}}=1.472$) is large (Cohen 1977; Hedges and Olkin 1985) demonstrating that the actual score of the overconfident sample is significantly lower than the score of the non-overconfident sample with $p=.000$. In fact, the overconfident group seems to have less knowledge about privacy than the non-overconfident group which provides evidence for the Dunning-Kruger-effect. To test if there are any differences with regard to gender (1=female; 2=male), we used a chi-square test of homogeneity. The mean and SD values for gender for each group are reported in Table 18. The result shows a non-statistically significant difference in proportions of .065, $p = .181$.

Table 18. Results of t-tests.

	Overconfident		Non-Overconfident		t-Test		
	Mean	SD	Mean	SD	t-value	df	p-value
Actual Privacy Knowledge	6.12	1.763	8.03	1.181	6.611	47.694	.000
Age	36.22	12.088	36.06	12.088	-0.770	237	.939
Privacy Experience	3.49	0.991	3.32	0.961	-1.008	237	.314
Gender	1.61	0.494	1.49	0.501	-1.338	58.345	.182

Discussion and Implications

Derived from the literature review of Kokolakis (2017), our research is the first to introduce overconfidence to the privacy calculus model by challenging its rational assumption. The goal of our research was (1) to uncover overconfidence in privacy knowledge, (2) investigate its effect on behavioral intention, and (3) explore group differences between overconfident and non-overconfident participants. In the following section we relate our findings to extant research and discuss its theoretical as well as practical implications.

Based on an empirical study including a privacy quiz among 239 internet users, we contribute to IS privacy research in several ways. We found evidence that the privacy calculus (Culnan and Armstrong 1999; Dinev and Hart 2006) is subject to overconfidence (Oskamp 1965; Russo and Schoemaker 1992). Overconfidence overrides the influence of privacy risks on disclosure decisions. It counteracts the rational assumption of the privacy calculus and thus contributes to recent literature arguing that users' lack rational decision-making when deciding whether to disclose personal information online (e.g., Brakemeier et al. 2017; Cho et al. 2010). Overconfident individuals are not aware what they do not know, because they think that they know more than they actually know (Russo and Schoemaker 1992). Subsequently, they overrate their own knowledge which interferes rational decision making.

By demonstrating that overconfidence moderates the relationship between privacy risks and intentions, we move beyond prior research indicating that overconfidence is an issue in privacy decision making (e.g., Jensen et al. 2005). Thereby, we provide a potential reason why the effect of privacy risks on intentions is controversial in recent literature relying on the privacy calculus (e.g., Kehr et al. 2015; Shibchurn and Yan 2015). Thus, only when individuals are aware of their fallibility when assessing their own competence, they can perform a rational tradeoff between benefits and risks, because they are less distorted by their own illusion of control. These results are in line with behavioral economics literature and its framing paradigm (Kahneman and Tversky 1979) which deems overconfident individuals to frame their risks positively, whereas other individuals frame it negatively which affects how benefits and risks are perceived. This is also reflected in the f^2 values, where it can be seen that in the overconfident group hedonic benefits have the greatest impact on the intention to use, whereas in the non-overconfident group risks are the most influential factor. In this light, we contribute to research building on behavioral economics by showing that overconfidence indeed distorts decision making and should in turn be assumed as a stable bias which varies across individuals (Glaser et al. 2013).

Surprisingly, the perceived utilitarian benefit of the application was not significantly related to behavioral intentions for the group of overconfident participants. This indicates that they were solely focused on hedonic aspects of the smartphone app. One potential explanation for this finding might be that the major motif to use apps is its playfulness and fun factor (Statista 2018b) which moves to the front for overconfident individuals as they are focused on their primary gains.

Apart from these findings, our results confirmed the existence of the rational privacy risk-benefit tradeoff for the group of non-overconfident participants. When individuals were not overconfident with regard to their privacy competence, privacy risks and benefits were both significantly related to behavioral intentions. Privacy risks were even found to be the most influential antecedent of the intention to use the application. This might clarify why the vast majority of information privacy research have found evidence for the rational privacy calculus to explain privacy decisions (Xu et al. 2009; Krasnova et al. 2010a; Li 2012). Furthermore, it contributes to scholars' arguing that internet users are overwhelmed when making self-disclosure decisions online (Korff and Böhme 2014).

Based on a representative sample with regard to gender, age and employment status for European internet users, we show that overconfidence bias in the privacy domain is independent of any investigated sociodemographic variable. Thus, our findings indicate that overconfidence is not an exclusive issue among certain populations. However, we provide evidence that the "Dunning-Kruger-effect" is present in our data: Those who are the least knowledgeable overestimate their competence the most (Kruger and Dunning 2002). It refers to individuals tendency to have high self-views which makes them feel at least as good as averaged others (Ehrlinger et al. 2008). This

finding might help explain why individuals are reluctant to read privacy policies (Smith 2014) or hesitate to engage in countermeasures (Dommeyer and Gross 2003), even though their knowledge of data practices is very low. The Dunning-Kruger-effect can be reduced by feedback (Ryvkin et al. 2012). However, feedback in real life privacy decision-making is very rare. Predominantly, data is collected and processed without individuals' awareness (Acquisti and Grossklags, 2005b) and beyond that most data breaches like identity thefts are not notified by users. Burson et al. (2006, p. 3) describe this phenomenon as the "unskilled-unaware hypothesis".

Beyond theoretical implications, our study offers practical implications for organizations, policy makers and especially end users. First, a firm aiming to make privacy a competitive advantage by providing sufficient safeguards, needs to be aware of customers' overconfidence in their own competences. Understanding distortions of potential users is essential to help users develop coping strategies for their perceived privacy risks and guide them to manage their risks accordingly. Thus, organizations can build on our results by sensitizing their customers that securing privacy is complex and thus requires a high level of knowledge and awareness. Second, our results might be of relevance for policy makers. Users of privacy-invasive systems are not always able to make rational decisions in accordance with their privacy preferences. Some overestimate their own competence and thus their ability to handle such risks. Therefore, policy makers are on duty to adopt regulations which mitigate users' risk of exploitation, because overconfident users are likely to disclose more information than they would actually do when they were aware of their irrationality. Lastly, users can learn from our results by being aware of their potential misperception regarding their competence. Ignoring their own overconfidence can cause unnecessary efforts, preventable privacy thefts and unintended data circulation, especially when transacting with malicious providers. When making a decision to disclose their data, they should question themselves whether they have sufficient competence to evaluate their own risks – not only in its extremity but also on their ability to handle that risk. In line with the Dunning-Kruger effect, this guidance is especially applicable for novices in the privacy domain.

Limitations and Future Research Suggestions

As with every research project, our study is subject to several limitations which should be taken into account when considering our findings. In order to measure overconfidence, it was necessary to capture individuals' actual privacy knowledge in a comprehensive and objective manner. Thus, in line with previous research (Ament 2017) we relied on a privacy quiz which was carefully compiled and pretested. Even though, the test difficulty and the privacy themes can be deemed as applicable for our investigation, other difficulty levels or privacy themes can lead to slightly different results (for review see Klayman and Gonza 1999). As we relied on a moderate difficulty level (as indicated by the mean of the perceived difficulty of 3.71 within our sample) and a broad range of privacy questions, we were trying to reduce this influence.

Smartphone applications were chosen as the optimal context to investigate privacy decision making. It allowed us to present participants a privacy-invasive information system which obviously collects, stores and processes personal information. Thereby, we relied on one set of personal information which was requested by the system. This set of personal information represents realistic requests (Olmstead and Atkinson 2015). However, this application along with its privacy requests counteracts generalizability of our results.

Although there are other approaches available, overconfidence was measured based on the overestimation formula (Moore and Healy 2008) with the help of a privacy quiz as suggested by

Russo and Schoemaker (1992). We measured overconfidence in an online survey with a fictive smartphone app in order to test whether overconfidence exists in privacy decision-making. It would be interesting to see whether overconfidence individuals actually disclose more information than non-overconfident individuals. In a consecutive project, we are aiming to move beyond the investigation of intentions by measuring actual behavior. Further, the robustness of overconfidence can be investigated by testing the influence of applicable debiasing tools like warning messages. Eventually, individuals might consider their perceived privacy risks when being aware of their illusory control over their privacy. Furthermore, future research can test antecedents of overconfidence in privacy knowledge.

Conclusion

In today's digitized society, privacy thefts are ubiquitous. In this vein, internet users are faced with the challenge to make sound decisions regarding their privacy. They have to rely on their own knowledge which can be distorted by overconfidence as one of the most critical bias in individuals' decision making. It exaggerates perceptions of ones' ability, chances of success and control in uncertain events. As such, it counteracts the assumption that individuals make a rational tradeoff between benefits and privacy risks when transacting with a Privacy-invasive information system provider. In fact, some individuals are "too confident to take care" of their privacy by moderating the effect of privacy risks on subsequent disclosure behavior. Interestingly, individuals who are the less knowledgeable are most at risk to become a victim of their own overconfidence. In contrast, non-overconfident individuals seem to act as rational agents weighing up their benefits and risks whereas risks are a major influential factor on their intention to use privacy-invasive systems.

8 Research Paper 3.A: Antecedents of Self-Disclosure on SNS

Title: Understanding Self-Disclosure on Social Networking Sites - A Literature Review

Authors: Abramova, Olga; Wagner, Amina; Krasnova, Hanna; Buxmann, Peter

Published in: Americas Conference on Information Systems (AMCIS), Boston, USA, 2017

Abstract

User-generated content is the backbone of any social networking site (SNS) and an important pillar of many business models online. While there is a growing body of research on self-disclosure on SNSs, existing insights remain scattered. To fill this gap, we undertake a systematic literature review by examining 50 studies to identify the factors behind self-disclosure on SNSs. We find that social exchange theory and its extension 'privacy calculus' represent a dominant theoretical perspective. Hence, we focus on perceived benefits and costs, as well as cost-mitigating factors as main areas of our investigation. Since personality traits are commonly controlled for or studied within the context of SNS disclosure, we additionally include an exploration of this factor group into our review.

Keywords: Self-Disclosure, Social Networking Sites, Literature Review.

Introduction

Social Networking Sites (SNSs) are successfully encouraging their users to disclose personal information. Every minute, numerous SNS users are commenting on pictures, share status updates and photos, and express their preferences by liking the content of others (Pew Research 2016). In the offline context, self-disclosure is typically defined as the divulgence of personal information from one person to at least another one (Wheeless and Grotz 1976) and is characterized by its voluntariness and uniqueness (Derlega et al. 1993). When disclosing, individuals intentionally reveal information that is not known to a designated audience. Disclosing personal information can be intrinsically rewarding (Tamir and Mitchell 2012). Moreover, perceived extrinsic benefits, such as relationship maintenance may motivate users to share (Aharony 2016). In addition, certain personality traits may have a favorable effect on users' intention to self-disclosure (Hollenbaugh and Ferris 2014). At the same time, self-disclosure decision is typically associated with various concerns, particularly privacy risks (e.g., Christofides et al. 2012; Kim et al. 2015; Krasnova et al. 2010a).

Although previous research has explored the determinants of self-disclosure decisions on SNSs, results remain confounding and scattered. For instance, while privacy concerns are often viewed as a major impediment to self-disclosure (e.g., Stutzman et al. 2011), some studies found no link between user privacy concerns and the information disclosed (e.g., Tufekci 2007). Second, a number of antecedents have been found to influence user willingness to share personal information on SNSs, ranging from personality traits, psychological states to perceived social benefits and privacy risks. The presence of this multitude of antecedents provides evidence for the complex nature of self-disclosure and the need for further research guidance in this field.

Given this background, in this study we conducted a structured literature review to analyze the extant research on the determinants of self-disclosure on SNSs. Building on the guidelines of von Brocke et al. (2009) and Webster and Watson (2002), we analyzed and synthesized relevant empirical studies in this area. In terms of research contribution, our study provides an initial attempt to synthesize existing research findings on the determinants of self-disclosure on SNSs. For SNS providers, our study provides a holistic view on how to better engage users to share and interact on SNSs.

Review Method

We conducted a structured literature review following the guidelines by von Brocke et al. (2009) and Webster and Watson (2002). In doing so, we retrieved relevant studies pertaining to the search topic which was defined as the "antecedents of self-disclosure on social networking sites". We performed searches within a one week period in February 2017 using the following scientific databases: ScienceDirect (420), EBSCOhost (125), ACM Digital Library (579), Wiley Online Library (9), JSTOR (31), IEEE (149) and Google Scholar (293) targeting the keywords: ((“disclosure” OR “self-disclosure” OR “disclose” OR “disclosing” OR “information sharing”) AND (“SNS” OR social networking site OR “Facebook” OR online social network OR “OSN”)) with a pre-defined ‘published within’ range of 1st January 2004-February 2017. After removing duplicates, the keyword search yielded 1445 papers for further screening. Next, titles and abstracts were reviewed. At this point, we relied on the following inclusion criteria: (1) studies should be published in English, (2) relationships should be empirically tested and (3) studies should be focused on self-disclosure as a dependent variable. Finally, full-text of remaining studies was reviewed. Articles were excluded according to the following criteria: (a) only descriptive data

without statistical analysis was provided; (b) focus on a very specific target group (e.g. depressive patients); (c) focus on a very specific type of relationships (teacher-student, employer-employee, doctor-patient); (d) no empirical focus on the antecedents of self-disclosure per se (e.g. investigation of cultural differences). As a result, 50 studies met our criteria. In terms of methodology, the overwhelming majority of studies (92%) in our sample have chosen a survey method to answer their research question. Other methods used included case study (Kim et al. 2016; Tzortzaki et al. 2016), experiments (Bazarova and Choi 2014; Ma et al. 2016) and data mining (Li et al. 2015). 18 studies investigated behavioral patterns of SNS users in general without platform specification. In 25 articles (50%) the sample consisted only of the members of the world's largest SNS – Facebook, and 3 papers focused on its Chinese counterpart - Renren.

Results

Theoretical Foundations

Based on our review we observed that past research has approached self-disclosure on SNSs using a variety of theoretical perspectives (Table 19). The most prevalent among them all is *social exchange theory* (SET), which conceptualizes SNS participation and self-disclosure as an outcome of a cost-benefit analysis (Ko and Chen 2009). Adopting this principle to the Information Systems context, *privacy calculus theory* (PC) attributes the 'costs' of disclosure mainly to privacy threats (Cheung et al. 2015; Krasnova et al. 2010a, 2012; McKnight et al. 2011; Ng 2014; Stern and Salb 2015). Further, *communication privacy management theory* (CPM) proposes that users set the limits of what they are ready to reveal (privacy boundaries) and coordinate them for different communication parties depending on the perceived benefits and costs of information disclosure (e.g., Chennamaneni and Taneja 2015; Li et al. 2015; Zlatolas et al. 2015). Focusing more on the positive aspects, *social capital theory* views self-disclosure on SNSs as an instrument to acquire and maintain mutually beneficial connections (Chen and Sharma 2013; Chen et al. 2016). Similarly, *uses and gratification theory* suggests that users share information to fulfil certain goals like gaining a specific gratification, such as enjoyment (Chang and Chen 2014; Hollenbaugh and Ferris 2014). Several studies build on the *theory of reasoned action* (TRA), which explains the relationship between attitudes and actual disclosure by the outcomes users expect as a result of engaging in self-disclosure (Kim et al. 2016). Complementing this framework with subjective norms and perceived behavioral control, *theory of planned behavior* (TPB) improves the predictive power of TRA (Lo and Riemenschneider 2010). Dealing with individual outcome expectations, which can be of any valence, TRA and TPB are used in combination with SET/PC to investigate self-disclosure in social networks (e.g., Shibchurn and Yan 2015; Stern and Salb 2015).

Table 19. Theoretical frameworks used to study self-disclosure.

Theory	SET/PC	TRA/TP	CPM	UG	SCaT	Other	No
Percentage of 50 papers (number)	18% (9)	10% (5)	6% (3)	4% (2)	4% (2)	20% (10)	42% (21)

Note: SET – Social Exchange Theory; PC – Privacy Calculus; TRA – Theory of Reasoned Action; TPB – Theory of Planned Behavior; CPM – Communication Privacy Management Theory; UG – Uses and Gratification Theory; SCaT – Social Capital Theory.

Other theoretical lenses used to understand the dynamics of self-disclosure on SNSs in studies we reviewed include *social cognitive theory* (Kim et al. 2015), *technology acceptance model* (Gupta and Dharmi 2015), *protection motivation theory* (Salleh et al. 2013), *functional theory of self-*

disclosure (Bazarova and Choi 2014), *similarity theory* (Hooi and Cho 2013), and *attachment theory* (Aharony 2016).

Measurement of Self-Disclosure

In most studies, self-disclosure was operationalized using a unidimensional instrument with different number of items measured on a Likert scale. One of the most popular scales was developed by Krasnova et al. (2010a) and further used by Krasnova et al. (2012), Kwak et al. (2014), Chen and Sharma (2013), Cheung et al. (2015), and Stern and Salb (2015). Examples of self-developed scales can be found in Wang and Stefanone (2013), Cheon et al. (2015) or Tzortzaki et al. (2016). Alternatively, some studies conceptualize self-disclosure as a multidimensional construct, and distinguish between frequency, depth and amount (Bevan-Dye and Akpojivi 2015); amount and accuracy (Chen et al. 2016); amount, depth and breadth (Hollenbaugh and Ferris 2014); breadth, depth and less sensitive/highly sensitive (Li et al. 2015); and amount, honesty, intent and positivity (Park et al. 2011). In some cases, self-disclosure was captured by a number of disclosed items (Stutzman et al. 2011), or indices were calculated as a number of disclosed items divided by a number of available items (Schrammel et al. 2009 a, 2009b).

Self-Disclosure Antecedents

Our systematic literature review reveals an array of antecedents that underlie individual disclosure behavior on SNSs, as tested and shown by prior research. Considering the cost-benefit perspective as the mainstream approach to explain user decision-making, we categorize dominant factors into four groups: self-disclosure benefits, self-disclosure costs, cost-mitigating factors, and personality factors.

Benefits of Self-Disclosure

Sharing personal information on SNSs is associated with a number of different benefits, as presented in Table 20. In line with the original purpose of online social communities, past studies deliver ample evidence that users share information on SNSs to gain relational benefits, including building new relationships (Cheung et al. 2015; Krasnova et al. 2010a; Park et al. 2011), maintaining existing ties (Bazarova and Choi 2014; Chennamaneni and Taneja 2015; Ng 2014; Park et al. 2011), and acquiring social capital (Aharony 2016; Tzortzaki et al. 2016); and are also motivated by the reciprocity within the community (Chen and Sharma 2013) and their need for affiliation (Chen et al. 2015, 2016). Interestingly, however, Chang and Chen (2014) found the impact of relationship management construct to be non-significant. Examining self-disclosure in a more granular way, Hollenbaugh and Ferris (2014) found that relationship maintenance predicts the amount and breadth, but not the depth of self-disclosure. At the same time, feeling as part of virtual community influences only the depth dimension of self-disclosure.

A number of studies provide evidence that sharing personal information is driven by pleasant feelings like enjoyment (Chennamaneni and Taneja 2015; Cheung et al. 2015; Kim et al. 2015; Krasnova et al. 2010a, 2012; Ng 2014) and entertainment (Bazarova and Choi 2014). Nonetheless, the study of McKnight et al. (2011) and Chang and Chen (2014) found this motive to be insignificant. Further, having a large number of friends and acquaintances in their network, users are motivated by self-presentation (Ng 2014), popularity (Chen et al. 2015; Christofides et al. 2009) and attention-seeking motives (Chennamaneni and Taneja 2015). The relevance of the self-presentation motive in predicting self-disclosure, however, is not confirmed by Krasnova et al. (2010a). Interestingly, exhibitionism contributed to the amount, but not to the depth and the breadth of self-disclosure in the study of Hollenbaugh and Ferris (2014).

Table 20. Benefits of self-disclosure.

Study	REL	EN	SE	SP	USE	GB	Other	Plat	M
Aharony (2016)	+							F	S
Ahmed (2015)								SNS	S
Bazarova and Choi (2014)	+	+	+					SNS	E
Chang and Chen (2014)	o	o						F	S
Chang and Heo (2014)						+		F	S
Chen and Sharma (2013)	+							F	S
Chen et al. (2016)	o							F	S
Chen et al. (2015)	+			+				F	S
Chennamaneni and Taneja (2015)	+	+		+			✓	SNS	S
Cheon et al. (2015)							✓	F	S
Cheung et al. (2015)	+	+		+				F	S
Christofides et al. (2009)				+				SNS	S
Hollenbaugh and Ferris (2014)	+/o			+/o			✓	F	S
Hooi and Cho (2013)							✓	SNS	S
Kim et al. (2015)	+	+						F	S
Ko and Chen (2009)							✓	B	S
Krasnova et al. (2010a)	+	+		o	+		✓	F	S
Krasnova et al. (2012)		+						B	S
Kwak et al. (2014)						+		F	S
Loiacono (2014)						+		R	S
McKnight et al. (2011)		o			o		✓	SNS	S
Ng (2014)	+	+		+			✓	F	S
Park et al. (2011)	+/o							SNS	S
Salleh et al. (2013)						+		F	S
Shibchurn and Yan (2015)					+		✓	SNS	S
Tzortzaki and Sideri (2016)	+							F	C

Note: REL – Relational benefits (including relationship maintenance, relationship building, social capital, affiliation, reciprocity); EN – Entertainment / Enjoyment; SE - Self-expression; SP -Self-Presentation (including attention-seeking, need for popularity); USE – Usefulness / Convenience; GB – General Benefits; Plat - Platform; F – Facebook; R – Renren; B – Blog; M – Method; S – Survey; C – Case Study; “+”-positive significant relation; “-”-negative significant relation; “o”-not significant relation; “+(-)/o” – significant/insignificant depending on the dimension of self-disclosure or construct operationalization; “✓” – other factors were also tested in the empirical model.

Other drivers to disclose on an SNS include self-expression as it allows for emotional relief (Bazarova and Choi 2014), perceived usefulness (Shibchurn and Yan 2015), convenience (Krasnova et al. 2010a) and passing time (Chennamaneni and Taneja 2015).

Costs of Self-Disclosure

Costs of self-disclosure can be described as perceived impediments negatively influencing users' decision to share information on SNSs (Table 21). Following our analysis, privacy concerns

(column 2, Table 21) fueled by user perceptions regarding improper data practices by an SNS provider or fears regarding unauthorized access to personal information are reported in a number of studies as the main impediment of individual disclosure decisions (Chang and Chen 2014; Chennamaneni and Taneja 2015; Hajli and Lin 2016; Krasnova et al. 2010a, 2012; Lo and Riemenschneider 2010; McKnight et al. 2011; Ng 2014; Stutzman et al. 2011; Zlatolas et al. 2015). There are, however, a few studies that found privacy concerns to be statistically insignificant in predicting user disclosure decisions (Cheung et al. 2015; Salleh et al. 2013; Tufekci 2007; Tzortzaki et al. 2016). Additionally, a number of studies found supporting evidence that SNS users refrain from self-disclosure as a result of perceived general risks (Loiacono 2014; Salleh et al. 2013; Shibchurn and Yan 2015). In contrast to privacy concerns, perceived general risks are defined broader and operationalized, e.g., as: “Overall, my perception of risk from using this SNS is low” (Loiacono 2015).

Table 21. Costs of self-disclosure and cost-mitigating factors.

Study	Costs				Cost-mitigating factors			Plat	M
	PC	PR	AC	Other costs	TR	CONT	Other CMF		
Aharony (2016)				✓				F	S
Bateman et al. (2011)							✓	F	S
Bevan-Dye and Akpojivi (2015)					+			SNS	S
Chang and Chen (2014)	–				o		✓	F	S
Chang and Heo (2014)		o			+			F	S
Chen and Sharma (2013)					+			F	S
Chen et al. (2016)					o			F	S
Chennamaneni and Taneja (2015)	–					+		SNS	S
Cheung et al. (2015)	o							F	S
Christofides et al. (2009)					o			SNS	S
Gupta and Dharmi (2015)					+	+	✓	F	S
Hajli and Lin (2016)	–					+		F	S
Hooi and Cho (2013)				✓				SNS	S
Kim et al. (2015)							✓	F	S
Kim et al. (2016)						+		SNS	C
Krasnova et al. (2010a)	–							F	S
Krasnova et al. (2012)	–				+			B	S
Lo and Riemenschneider (2010)	–				+		✓	F	S
Loiacono (2014)		–						R	S
McKnight et al. (2011)	–			✓	–			SNS	S
Mital et al. (2010)					+			SNS	S
Ng (2014)	–							F	S
Salleh et al. (2013)	o	–			+			F	S
Schrammel et al. (2009a)					+		✓	F	S

Schrammel et al. (2009b)					+			SNS	S
Shibchurn and Yan (2015)		–						SNS	S
Stern and Salb (2015)						+		SNS	S
Stutzman et al. (2011)	–					+/o		SNS	S
Tufekci (2007)	o		o					SNS	S
Tzortzaki and Sideri (2016)	o							F	C
Xie and Kang (2015)				✓				F	S
Zhao et al. (2012)						+		SNS	S
Zlatolas et al. (2015)	–						✓	R	S

Note: PC – Privacy concerns; PR – Perceived (general) risk; TR – Trust in the platform or community; CONT – Control over access/privacy setting; AC – General audience concerns; Other CMF – other cost-mitigating factors.

Tightly linked to user privacy concerns, Tufekci (2007) separately points out audience concerns as a possible impediment to self-disclosure: However, empirical analysis does not reveal significant influence of this factor. Moreover, although not included in our literature sample, qualitative analysis of interviews in the study of French and Read (2013) shows that the overwhelming majority of users apply blocking functions to prevent unwanted people from observing their content. One possible reason for this is that users might feel better when they know certain people or social circles are unable to see their posts (French and Read 2013). Beyond privacy concerns, and perceived general risks, other factors, including information sensitivity (McKnight et al. 2011), insecurity (Aharony 2016), and identifiability (Hooi and Cho 2013) were recognized as additional inhibitors of self-disclosure (column 5, Table 21).

Cost-Mitigating Factors

Inconsistency in empirical results regarding the role of privacy concerns in user self-disclosure decisions can be partly explained by the presence of contextual cost-mitigating factors (Table 21). Among others, control emerges as an important facilitating condition (Hajli and Lin 2016; C. Zhao et al. 2012): For example, Stern and Salb (2015) show that privacy settings can be used to mitigate privacy-related costs of self-disclosure. In addition, other control-related factor, such as customization is shown to decrease user perceptions of risks (Stutzman et al. 2011). However, personalization and reading Facebook privacy policies was shown to be insignificant (Stutzman et al. 2011). Trust emerges as another most common cost-mitigating factor. Tested as trust in online community (Chang and Heo 2014; Lo and Riemenschneider 2010; Schrammel et al. 2009a,b; Zhao et al. 2012), trust in members (Bevan-Dye and Akpojivi 2015; Krasnova et al. 2012), trust in provider (Krasnova et al. 2012) and general trust (Gupta and Dhami 2015; Mital et al. 2010; Salleh et al. 2013), trust was found to contribute to self-disclosure. Exceptions include studies by Christofides et al. (2009) and Chang and Chen (2014), in which trust was not found to be significant in facilitating self-disclosure decisions. Further, factors, such as perceived publicness (Bateman et al. 2010), perceived privacy (Gupta and Dhami 2015), perceived privacy control (Chang and Chen 2014), perceived security (Gupta and Dhami 2015; Kim and Lee 2015), privacy value (Zlatolas et al. 2015) were categorized as “other cost-mitigating factors” that also play a role in self-disclosure decisions of users on SNSs.

Personality Factors

Included in 17 studies in our sample, personality factors may also have an impact on self-disclosure behavior.

Table 22. Personality factors and their relation to self-disclosure.

Study	SE	Agr	Con	Ext	Neu	Op	Narc	Other PF	Plat	M
Aharony (2016)				+		o			F	S
Błachnio et al. (2016)								✓	F	S
Chen et al. (2015)	+	-	-	o	+	-			F	S
Christofides et al. (2009)	o								SNS	S
Hollenbaugh and Ferris (2014)	o/-	o	o	o/+	o/-	o/+		✓	F	S
Hooi and Cho (2013)	o								SNS	S
Kim et al. (2015)								✓	F	S
Kim et al. (2016)							+		SNS	C
Ko and Chen (2009)	+							✓		S
Li et al. (2015)									F	DM
Loiacono (2014)		-	o	+	-	o			R	S
Pentina and Zhang (2016)		o/+	o/-	o/+	o	o		✓	F	S
Schrammel et al. (2009a)		o		o	o	o			SNS	S
Wang and Stefanone (2013)				+			o		SNS	S
Xie and Kang (2015)									F	S
Yu and Wu (2010)				-				✓	F	S
Zhang and Ling (2015)		+		+			+	✓	SNS	S

Note: SE – Self-Esteem; Agr – Agreeableness; Con – Conscientiousness; Ext – Extroversion; Neu – Neuroticism/Instability; Open – Openness; Narc – Narcissism; Other PF – other personality factors; DM – Data Mining.

Often measured with the help of Big Five Inventory (extraversion, agreeableness, conscientiousness, neuroticism, and openness), empirical testing of personality traits delivers mixed evidence (Table 22). For example, studies by Aharony (2016), Loiacono (2014), Wang and Stefanone (2013), Zhang and Ling (2015) found that extraversion encourages information sharing on SNSs. This proposition, however, is only partially supported in studies by Pentina and Zhang (2016) and Hollenbaugh and Ferris (2014). Furthermore, studies by Chen et al. (2015) and Schrammel et al. (2009a) found no evidence of this link; and study by Yu and Wu (2010) found an association in a negative direction.

Tested by Kim et al. (2016) and Zhang and Ling (2015), narcissism is shown to boost disclosure intentions. Further, self-esteem is positively linked to self-disclosure in studies by Chen et al. (2015) and Ko and Chen (2009), but is reported as insignificant by Christofides et al. (2009), Hollenbaugh and Ferris (2015) and Hooi and Cho (2013). Finally, a few studies test such psychological states as loneliness (Błachnio et al. 2016; Zhang and Ling 2015), emotional stability (Pentina and Zhang 2016), and subjective well-being (Ko and Chen 2009) as antecedents of self-disclosure. These factors are pooled in the category “other PF” (column 9, Table 22). Taken

together, our review suggests that research evidence on the role of personality traits in individual self-disclosure is still inconclusive.

Discussion

The goal of this systematic literature review was to examine existing state of research concerning the factors behind individual self-disclosure on SNSs. Fifty papers were analyzed to gain insight into motivations and inhibitors of information sharing among SNS users. Our review reveals that social exchange theory and its extension in the form of ‘privacy calculus’ model have been the most frequently used theoretical lens to explain user decisions to share personal information on SNSs. This theoretical perspective views self-disclosure as a cognitive process, in which users weigh costs and benefits of their disclosure, and act accordingly (Cheung et al. 2015; Krasnova et al. 2010a, 2012; McKnight et al. 2011; Ng 2014; Stern and Salb 2015). All in all, more than 15 different theoretical approaches have been employed in the studies in our sample. Surprisingly, in 21 (42%) studies no theoretical foundation was used. In many cases, such studies focus on a specific set of factors researchers found interesting (e.g., psychological traits, tie strength, etc.).

To provide a better overview of factors influencing self-disclosure on SNSs, four groups of factors were derived: namely, (perceived) benefits and costs of self-disclosure, cost-mitigating factors and personality factors. In terms of benefits, we found that users are mainly driven by relational benefits such as starting new relationships or maintaining existing ones, need of affiliation and reciprocity (e.g., Krasnova et al. 2010a; Park et al. 2011; Chennamaneni and Taneja 2015). Enjoyment (e.g., Ng 2014; Cheung et al. 2015; Kim et al. 2015) and self-presentation (e.g., Christofides et al. 2009; Chennamaneni and Taneja 2015; Chen et al. 2015;) also emerge as important motives of self-disclosure. Costs of self-disclosure are typically subsumed under the notion of privacy concerns, which are often linked to SNS provider, audience or third parties (e.g. Krasnova et al. 2010a; 2012; Hajli and Lin 2016; McKnight et al. 2011; Zlatolas et al. 2015). At the same time, past research finds that trust (Chang and Heo 2014; Lo and Riemenschneider 2010; Zhao et al. 2012) and control in the form of privacy settings (e.g. Stutzman et al. 2011) may lessen privacy concerns – a group of factors we refer to as “cost-mitigating” (Cheung et al. 2015). Tested in a number of studies, the influence of personality traits on user self-disclosure remains ambiguous (e.g., Chen et al. 2015; Hollenbaugh and Ferris 2014; Pentina and Zhang 2016).

Conclusion, Limitations and Future Research Suggestions

Disclosure of personal information is an integral part of any social networking community. As a result, multiple studies focus on exploring the reasons underlying individual self-disclosure decisions on SNSs. However, empirical results remain scattered. This paper addresses this gap by conducting a systematic literature review and providing a comprehensive summary of existing findings into the factors behind individual self-disclosure decisions on SNSs.

This study makes a number of contributions to research and practice. Summarizing extant research, this study provides a structured review of current literature on self-disclosure on SNSs with a special focus on its antecedents. Among others, we reveal an array of conflictual findings that exist in the literature, which calls for more exploration into the reasons of these diverging insights. Overall, our study could serve as a starting point for future research in this area. For SNS providers, this research points out the drivers and inhibitors of self-disclosure, as well as identifies factors that mitigate concerns of SNS users. Building on our insights, SNS providers could better understand the dynamics of information sharing on their platforms, and ethically use

this knowledge to motivate users to further contribute to the network. This is important since user-generated content is the backbone of any online community and many business models online. Among others, SNS providers could focus on offering personalization and customization features to enable users with better control over their audience size and access to personal information, which is likely to mitigate user privacy concerns and enhance trust, thereby facilitating user engagement on the platform.

Current study has several limitations. First, studies in our sample are a result of a keyword search, followed by subsequent exclusion. Second, the overwhelming majority of studies in our sample investigate benefits from a “rational” perspective, assuming that users cognitively weigh their options and act accordingly. Recognizing these limitations, future research may provide a more comprehensive review of extant body of research by completing the backwards and forward search procedures that may increase the sample and reveal additional insights. Moreover, we encourage future research to conduct a meta-analysis to summarize existing results with the help of statistical methods. Finally, since a growing body of literature hints at the presence of cognitive distortions in human decision-making (Acquisti et al. 2015), it may be interesting to develop a holistic approach to account for both rational and “non-rational” thinking when exploring disclosure behavior on SNSs.

9 Research Paper 3.B: From Privacy Calculus to Social Calculus

Title: From 'Privacy Calculus' to 'Social Calculus': Understanding Self-Disclosure on Social Networking Sites

Authors: Wagner, Amina; Krasnova, Hanna; Abramova, Olga; Buxmann, Peter; Benbasat, Izak

Published in: International Conference on Information Systems (ICIS), San Francisco, USA, 2018

Abstract

This study extends the privacy calculus by a social perspective building on interpersonal communication theory along with the act of perspective-taking in the Social Networking Sites context. Based on a two-step study, we provide evidence for the presence of perspective-taking in self-disclosure decisions using a qualitative approach and empirically test the influence of anticipated perceptions for others on subsequent self-disclosure decisions among 231 Facebook users. Our results show that SNS users are less egoistic as typically assumed by the privacy calculus model guided by an intrapersonal tradeoff between own benefits and concerns. Users are tensed between their pleasure of self-enhancement and others' anticipated perception caused by their own behavior. However, although users think about the relevance of their message for others, their concern about others' negative affect is self-focused as it does not directly relate to self-disclosure intent. It is mediated by a fear of being negatively evaluated by others.

Keywords: Social Networking Sites, Privacy Calculus, Social Calculus, Perspective-taking, Interpersonal Communication.

Introduction

With Facebook alone counting more than 2.23 billion users worldwide (Statista 2017b), the role of Social Networking Sites (SNSs) as communication marketplaces cannot be ignored. Since user-generated content is the backbone of SNS business success, users are enticed to share more information with others. With 80% of users focusing on the self in their disclosures (Naaman et al. 2010), most SNS updates revolve around positive experiences, such as travel, major life events, child development progress, restaurant visits (Denti et al. 2012; Marshall et al. 2015), and good deeds (Berman et al. 2015). Considering the sheer scale of ongoing sharing, understanding psychological mechanisms behind individual disclosure decisions has been an important subject in the SNS research discourse (e.g., Barasch and Berger 2014; Fox and Moreland 2015).

So far, extant studies on self-disclosure on SNSs have been mainly based on social exchange theory in general and privacy calculus theory in particular (Abramova et al. 2017). These theoretical foundations postulate that decisions are based on a subjective evaluation of benefits and costs (Homans 1958). Following this perspective, self-disclosure decisions are a function of personal benefits and personal risks anticipated by users. On the positive side, users appear to be motivated by such benefits as the ability to stay connected with friends (e.g., Hollenbaugh and Ferris 2015), enjoyment (e.g., Krasnova et al. 2010a), as well as self-enhancement (Utz et al. 2012). On the negative front, studies have mainly adopted a privacy calculus lens, viewing privacy concerns as the major and in most cases the sole impediment to self-disclosure (e.g., Chang and Chen 2014; Krasnova et al. 2010a). According to this view, users weigh personal benefits they expect to obtain against the personal risk of privacy loss as a result of their self-disclosure, and act accordingly. In this context, the privacy calculus represents an intrapersonal tradeoff, only incorporating self-oriented antecedents.

However, an established body of research challenges this one-sided focus on intrapersonal costs and gains (Berlo 1960; Buller and Burgoon 1996; Westley and MacLean Jr 1957). They all lean on interpersonal communication research which is concerned with how people communicate and thus decide to disclose information to others (Buller and Burgoon 1996). Specifically, it suggests that when it comes to face-to-face interactions individuals continuously monitor their social environment and adjust their communication accordingly in the process referred to as perspective-taking (Epley et al. 2004; Galinsky et al. 2008; Leary 1999). In other words, not only do individuals consider their personal benefits and risks, but also those of “others” – their recipients. Perspective-taking reflects efforts of interaction partners to regulate their communication in response to their anticipation of the other’s reaction. Hence, it is assumed that senders construct their message in line with the needs and interests of their audience in order to achieve successful social communication (Buller and Burgoon 1996). For example, while people usually aim to produce the best impression possible, they often choose to remain modest and downplay their achievements to stay “likable” to their interaction partners (Leary 1999). Even though we know that perspective-taking helps to maintain successful communication, so far it remains unclear whether users account at all for outcomes and perceptions of others when contemplating their self-disclosure decisions on SNSs. In this vein, we address the following research questions: Do senders at all care about subsequent perceptions of others when communicating on SNSs? And if so, in which way do these perceptions influence self-disclosure decisions?

While interpersonal communication literature (Berlo 1960; Van Boven and Loewenstein 2005; Buller and Burgoon 1996) strongly suggests a critical role of considering “others”, only few

studies integrate this perspective when studying self-disclosure in SNS contexts (e.g., James et al. 2017; Min 2016; Yu et al. 2015). Studies building on impression management have touched upon this phenomenon by providing evidence that users are aiming to elicit positive emotions in others in order to be perceived favorably (Ellison et al. 2006; Oh and Larose 2016; Qiu et al. 2012). Other studies, however, claim that SNSs promote egocentricity, so that resulting communication is self-centered and less empathetic (e.g., Barasch and Berger 2014; Utz et al. 2012).

In order to answer our research questions, in this study we build on empirical evidence of (1) a qualitative pre-study that provides evidence for the presence of perspective-taking in self-disclosure decisions, and (2) a quantitative study with 231 Facebook users that tests the influence of anticipated perceptions and outcomes for others like expected negative affect of others on subsequent self-disclosure decisions. On the theoretical front, we build on the interpersonal communication and perspective-taking literature to investigate mental processes behind self-disclosure decisions on SNSs (Berlo 1960; Van Boven and Loewenstein 2005). Thereby, we extend the privacy calculus perspective prevalent in current research discourse. Specifically, we complement the intrapersonal trade-off between own benefits and privacy concerns extensively studied so far, with an interpersonal trade-off that arise when users try to engage in perspective-taking. By gaining a more in-depth understanding of mental processes underlying self-disclosure decisions, we show that active users of SNSs are less self-focused than previously thought.

Theoretical Background

Self-Disclosure on Social Networking Sites

Defined as the “process of making the self known to others” (Jourard and Lasakow 1958, p. 91), self-disclosure is a critical component of interpersonal relationships. Multidimensional in nature, self-disclosure can be analyzed from a number of angles, including its intentionality, amount, honesty, depth as well as positivity (Wheless and Grotz 1976). Especially the latter is salient in the context of SNSs, with research consistently providing evidence of users posting self-promotional content on the network (Mehdizadeh 2010; Peluchette and Karl 2009). For example, a study by Denti et al. (2012) found that 77.3% of Facebook users focus on positive things in their sharing. Against this background, in this study we focus on self-disclosure of positive information about the self which is intentionally revealed on the platform. This way the scope of our study encompasses one of the most common sharing practices on SNSs.

The theoretical foundations of self-disclosure go back to social exchange theory (Homans 1958). Social exchange theory remains a dominant perspective to theorize self-disclosure in the SNS discourse (Abramova et al. 2017), in which it is mainly interpreted within the framework of privacy calculus (Culnan and Armstrong 1999; Dinev and Hart 2006). Following this approach, one stream of SNS studies directly focuses on the intrapersonal benefits of disclosure decisions. Here, personal convenience, such as being able to effectively communicate with friends (Krasnova et al. 2010a) and private pleasure (Bazarova and Choi 2014; Yu et al. 2015) have been shown to be especially powerful in motivating users to reveal their information. Extending these findings with the cost perspective, other studies focus on privacy concerns, which are typically captured within the domain of organizational practices (Smith et al. 2011; Xu et al. 2011a). Hence, disclosure is modeled as an outcome of an intrapersonal trade-off in which users weigh the personal benefits and privacy concerns of their disclosures and act accordingly.

SNSs, however, reflects interpersonal communication where users share information with each other and thus puts them in a social position (Min 2016; Yu et al. 2015). In this vein, users share

information about themselves in a variety of ways on SNSs, ranging from revealing their preferences via a 'like' button, to sharing their personal 'status updates' and photos in order to stay connected (Johnston et al. 2011) and impress others (Mehdizadeh 2010). Thus, self-disclosure decisions on SNSs should also include a strong social component, which goes beyond intrapersonal concerns and benefits assumed in prior SNS research. Indeed, research on interpersonal communication emphasizes the importance of social thoughts in individual communication (Westley and MacLean Jr 1957), challenging the one-sided focus on solely intrapersonal factors. Specifically, it suggests that when it comes to social interactions individuals typically go beyond evaluating just intrapersonal factors, but also account for interpersonal benefits and risks in their communication with others - the process referred to as perspective-taking (Epley et al. 2004; Galinsky et al. 2008; Leary 1999).

Hence, in addition to a 'privacy calculus' perspective that focuses on user's intrapersonal benefits in exchange for personal information (e.g., Krasnova et al. 2010a), this article aims to integrate another layer of decision-making - 'social calculus'. In this vein, we move beyond the sole focus on the misuse of personal information by third parties as an impediment of disclosure. Specifically, we acknowledge the importance of interpersonal concerns and fears one might have with regard to others. In other words, the 'social calculus' perspective highlights how the sender anticipates perceptions and opinions of others, and how these perceptions shape individual decisions to share on the network (Leary and Kowalski 1990). Building on this conceptualization, in the following we draw on the theory of interpersonal communication along with the process of perspective-taking to extend the 'privacy calculus' approach typically applied in SNS research.

Perspective-Taking in Interpersonal Communication

Following interpersonal communication theory, self-disclosure influences the way others perceive, evaluate, and subsequently treat the sender (Buller and Burgoon 1996). Therefore, individuals engage in perspective-taking - the act of seeing the world from another's viewpoint (Epley et al. 2004). This way they seek to predict the outcomes of their self-disclosures on the recipient side (Galinsky et al. 2008), which helps them to maximize social approval, while avoiding social disapproval (Leary 1999). In this vein, they assess the success or failure of their message production by navigating triggered impressions, emotions and perceptions beneficial for the sender and the receiver (Buller and Burgoon 1996). For example, an empirical study of Wagner et al. (2018b) has shown that the success of self-disclosure decisions is depending on users' accurate anticipation of recipients' perception. Especially when it comes to disclosing positive information about oneself, self-disclosure emerges as a delicate act of balancing conflicting perceptions of receiving audiences. While sharing positive information allows a sender to show him-/herself in the best light possible in front of others, it also carries the risk of being perceived as arrogant or conceited, leading recipients to experience such undesirable reactions as feelings of envy, anger or irritation (Lange and Crusius 2015; Scopelliti et al. 2015). To assess these risks, users should implicitly care about the reactions triggered and emotions evoked in the receiving audience (Buller and Burgoon 1996).

While considering others (perspective-taking) is a common practice in interpersonal communication offline (Westley and MacLean Jr 1957), there is little research about the extent to which SNS users account for their audiences when communicating on the platform (Wagner et al. 2018b). In fact, analysis of available findings on technological affordances of SNS platforms, current practices and indirect empirical evidence offer a conflicted picture about the extent of perspective-taking that is taking place on the network. On the one hand, SNS environment implies communication to a wider audience, which is likely to motivate users to consider interests and

needs of others in their self-disclosures. This is because people get increasingly anxious when self-presenting in public since they worry about how they are perceived by their audience (Leary and Kowalski 1990b). These concerns subsequently motivate them to control for the perception of others, forcing them to “put their best foot forward” (Hancock and Toma 2009, p. 322). Importantly, SNS platforms offer users a number of tools to achieve these goals. For example, asynchronous nature of communication on SNSs, combined with features that enable users to post, edit, and hide content empower users with a high level of control over their content, motivating more strategic self-portrayals (Ellison et al. 2006). Additionally, SNS platforms offer functionalities like filters and picture-editing tools in order to present oneself in the best light (Hu et al. 2014). It helps users to construct a desired social image with less unconscious verbal or mimical expressions available to others (Walther 1996). Indeed, SNS research is abundant with studies demonstrating that users try to project socially desirable identities (Zhao et al. 2008), self-censor their contributions based on audience concerns (Sleeper et al. 2013), and try to impress their audiences (e.g., Peluchette and Karl 2009). Thus, being able to invest time and effort in message construction, perspective-taking should be leveraged on SNS.

On the other hand, there is mounting research evidence about the growing disconnect between senders and recipients on SNSs, which questions whether and to what extent perspective-taking is taking place on SNSs. For example, recipients report a feeling of fatigue from the staggering amount of information shared by their friends (Bright et al. 2015). Further, shared content seems to trigger a multitude of negative emotional reactions among its recipients, including feelings of envy, anger, and even contempt (Krasnova et al. 2015). A number of factors may work against users’ motivation to engage in perspective-taking on SNSs. For example, social norms prevalent on SNSs legitimize sharing of self-promotional content, motivating users to share most positive information about themselves (Peluchette and Karl 2009). As a result, posted images, selfies, and ideal depictions of life experiences are common on Facebook, and especially Instagram (Lyu 2016; Utz 2015), which inadvertently produces envy in others (Krasnova et al. 2015). Recent research underpins this evidence by indicating that communicating online leads to psychological distance causing egoism and lowered social concerns (Carrier et al. 2015). Further, feedback cycle is skewed towards positive reactions (‘likes’) on SNSs. Hence, even though a specific message might be ill-received by the audience, common reaction in the form of ‘likes’ is likely to reinforce the sender in the appropriateness of the content (Lee et al. 2016). Additionally, since self-presentation online is inherently impersonal, users are less likely to notice if their self-presentation attempts are being rejected or criticized (Walther 1996). Thus, they may be less sensitive to how their self-presentation attempts are being perceived by others.

Overall, the evidence on the extent of perspective-taking on SNSs remains mixed. Considering these platform specifics, it becomes unclear whether, senders at all care about (subsequent perceptions) of others when disclosing content on SNSs. To answer this research question, in this study we investigate whether and to what extent users integrate perceptions and emotions of others when sharing positive information on the network. Following the logic of social exchange theory, we extend the current perspective on the determinants of self-disclosure, namely ‘privacy calculus’, with an interpersonal focus.

Qualitative Pre-Study: Self- vs. Other-Focus

To better understand the nature and magnitude of perspective-taking on SNSs, we conducted a qualitative pre-study among active Facebook users. The aim of the pre-study was to test whether SNS users think about others when sharing content on an SNS. We distributed an online survey to

Facebook users. First, we granted our survey participants that their data will be treated anonymously. As the majority of posts on SNS are positive and self-expressive in nature, we asked participants to think about a recently experienced positive event. To be able to control for the type of event, participants were provided with an open text field to briefly describe it. After that, we asked the participants to explain 1) “What speaks against sharing your positive event on Facebook?” and 2) “What speaks for sharing this positive event on Facebook?” in order to gain a deeper understanding into the drivers and inhibitors of sharing with regard to others. 207 respondents from Germany participated in our survey. The majority were students (141) with a mean age of 26.6. 71.5% (148) were female and 28.5% (59) were male. In terms of positive events 25% of our respondents were thinking about their latest vacation while 22% were describing a professional accomplishment, such as, graduation or job promotion. All other events were grouped around the categories family and friends (17%) (e.g., new born baby), romantic time with partner (10%), general event (7%), products (6%), sport (6%) and positive other (7%) with statements like “a new shop has opened”.

In the next step, the antecedents of self-disclosure were subsumed, coded and linked to established research. Following methodological guidelines for qualitative studies of Ryan and Bernard (2000), we derived a preliminary set of categories on the basis of privacy calculus determinants identified in previous research (Abramova et al. 2017), as well as in the process of open coding. To trace the magnitude of perspective-taking, we specifically screened our dataset for words indicating “other”-focus (Miles and Huberman 1994). Two independent researchers coded all quotes and assigned them to the categories of our coding scheme. Multiple codes were possible per response. As we defined our coding table very comprehensively against the background of extant research, inter-coder reliability was also strong and beyond chance (average κ of 0.81) (Haley and Osberg 1989). Disagreements between coders were resolved by consensus. Table 23 provides a summary of influential determinants of self-disclosure decisions, frequency of answers and example answers.

As summarized in Table 23, in line with previous research investigating self-disclosure as a function of individual privacy calculus, “privacy concerns”, “convenience of communication with friends” and “self-enhancement” emerged as relevant intrapersonal determinants of self-disclosure decisions. While respondents anticipated the pleasure of self-enhancement, they expressed a distinct “fear of being negatively evaluated by others”, and consequently suffer from an image loss. In particular, they pointed out: “the post could be perceived as boastful”, or “the post can be misunderstood as showing off”. Thus, this impediment of self-disclosure is anticipated when there is a gap between individual’s self-image and the image which is presented on SNS through a certain posting (Lee et al. 2013).

With regard to “other”-related factors, two categories have been particularly salient in our dataset: “value of information for others” on the benefit side, as well as “negative affect of others” on the cost side. Specifically, respondents in our sample emphasized the “value of information” they intended to share “for others”, which emerged as the most important determinant of sharing decisions (relative quote count 43%). Here, a distinction between utilitarian (usefulness) and hedonic (visual appeal) value of the shared content was noticeable. For example, addressing the former, respondents stated: [I would share it] “(...) because the restaurant was very good there, as a tip for others” and “(...) to show to friends that there are very nice travel destinations in Europe”. Emphasizing the hedonic component, statements like “The pictures of the mountain lake could also please others” were salient. Overall, the importance of the category “value of

information” for others by a share of 43% in our dataset suggests that users prioritize the benefits of others when making self-disclosure decisions.

Beyond interpersonal benefits, respondents’ social concerns have been strong as well. Respondents were fearful that sharing specific content is likely to result in “negative affect” for others, suggesting that respondents engaged in the process of perspective-taking on the network. Within this category, respondents were largely concerned about the envy of others: “It could possibly cause envy because I was on vacation again.” Following envy, feelings of resentment and frustration (“other students who have not yet submitted their bachelor thesis could be frustrated”) and irritation (“others might be irritated or annoyed”) were pointed out. Interestingly, being concerned about the negative affect of others, and as a consequence fearing a negative evaluation by others in terms of image loss were often mentioned in combination, which suggests an association between both categories. This is in line with existing research that shows that feelings of envy are strongly associated with hostility as well as the desire to hurt the target (e.g., Cohen-Charash 2009).

Table 23. Summary of pre-study results.

Determinants of Self-Disclosure	Category Definition	Relationship to Existing Literature	Example Quotes from Respondents
<i>Intrapersonal Determinants: Self-Focus</i>			
Convenience of Communication with Friends (Benefit) 31%	“The value users derive from being able to efficiently and easily stay in touch with each other” on OSNs” (Krasnova et al. 2010a, p. 112).	Deductively derived from literature (for review see Chennamaneni and Taneja 2015; Cheung et al. 2015; Krasnova et al. 2010a)	“I can update friends who live abroad.” “It is an easy way to let all my friends know that I’m in the city.”
Self-Enhancement (Benefit) 42%	The pleasure “users derive from being able to improve their self-concept in relation to others using OSNs” (Krasnova et al. 2010a, p. 112).	Deductively derived from literature (for review see Cheung et al. 2015; Krasnova et al. 2010a, 2017)	“I am proud that I achieved it.” “To be in the center of attention.” “(…) to present my extraordinary experience.”
Negative Evaluation by Others (Cost) 19%	Self-related fear of an unwarranted social image on others (Lee et al. 2013; Savitsky et al. 2001).	Inductively derived from the pre-study	“The post can be misunderstood as showing off, because not everyone can afford such a semester abroad.” “I could be perceived as arrogant.”
Privacy Concerns (Cost) 50%	Concerns about possible loss of privacy as a result of information disclosure “to organizational entities” (Xu et al. 2008, p. 4).	Deductively derived from literature (for review see Chennamaneni and Taneja 2015; Cheung et al. 2015; Krasnova et al. 2010a)	“I’m not sure what Facebook will do with this information.” “I don’t want Facebook to have the right over my pictures.”

<i>Interpersonal Determinants: "Other"-Focus</i>			
Utilitarian and Hedonic Value of Information for Others (Benefit) 43%	Anticipation of others' attitude towards the shared message (Voss et al. 2003).	Inductively derived from the pre-study	"Great location that could be of interest for others." "The pictures of the mountain lake could also please others"
Negative Affect of Others (Cost) 13%	Concerns about causing negative emotional response in others (also referred to as the ability of emotional perspective-taking) (Leith and Baumeister 1998)	Inductively derived from the pre-study	"It could possibly cause envy because I was on vacation again." "Other students who have not yet submitted their bachelor thesis could be frustrated."

Finally, some statements (9%) were unique like "I use Facebook only passively", or "I have no desire to share it". This category was called "Other" and was excluded from further analyses due to its irrelevance.

To conclude, while our pre-study findings confirm the presence of 'privacy calculus' in individual decision-making, they simultaneously call for the extension of this paradigm with interpersonal determinants – the collection of mental processes involving perspective-taking we refer to as 'social calculus'. Specifically, following our results, 'social calculus' is based on user's assessment of (a) the value others will obtain from the shared information in terms of its hedonic and utilitarian dimension, as well as (b) concerns regarding the negative feelings others may experience when viewing it. Together, these findings are used as a baseline for our main empirical study. Against this background, we formulate our hypotheses accordingly.

Hypotheses Development and Research Model

Figure 11 depicts the extension of the privacy calculus by interpersonal antecedents for self-disclosure.

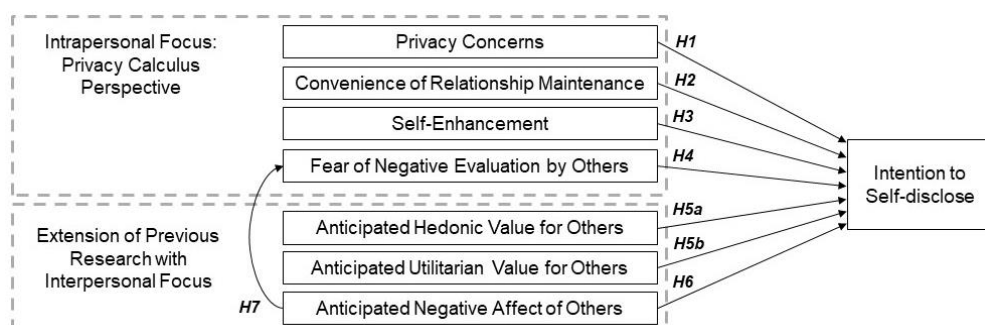


Figure 11. Conceptual research model.

Based on the privacy calculus model (Culnan and Armstrong 1999; Dinev and Hart 2006), extant SNS research largely assumes that users assess an intrapersonal tradeoff between anticipated benefits and privacy concerns and act accordingly (for review see Li 2012). Stemming from the perceived loss of control over ones' personal information (Smith et al. 2011; Xu et al. 2011a), privacy concerns have been shown to lower the intent to self-disclose on SNSs. In other words,

users who are concerned about how SNS providers will use or protect shared information will be less willing to share personal information on their platforms (see quotes of pre-study). Regardless of these concerns, users obtain certain benefits in exchange for revealing private information on the network. A comprehensive literature review by Abramova et al. (2017) points out "convenience of relationship maintenance" as a particularly salient determinant of self-disclosure in the SNS context. Convenience of relationship maintenance is referred to the extent to which SNSs are seen as effective in helping users stay in touch with each other (Krasnova et al. 2010a). Further, the review suggests that self-enhancement is a critical determinant which describes the pleasure users derive from being able to share information of which they are proud of and helps to improve their self-concept (Krasnova et al. 2010a; Exline et al. 2004). Clearly, these benefits are likely to drive self-disclosure on SNSs. Hence, we hypothesize according to the privacy calculus model:

H1: Privacy Concerns are negatively related to the intention to disclose information on an SNS.

H2: Convenience of relationship maintenance is positively related to the intention to disclose information on an SNS.

H3: Self-enhancement is positively related to the intention to disclose information on an SNS.

Research into symbolic behavior argues that any act of positive sharing can be situated along the competitive and the fear axis (Foster 1972). The competitive axis reflects private pleasure of self-enhancement individuals experience when presenting their desired image to others (Exline and Lobel 1999). Feelings of being proud and being able to present one's accomplishments to others are at the core of this experience (Lange and Crusius 2015), as reflected in H3 above. On the flipside, however, sharing positive news may lead others to perceive the sender as superior, selfish or arrogant – concerns reflective of the fear axis (Berman et al. 2015; Foster 1972; Lange and Crusius 2015). The salience of this interpersonal trade-off is exemplified by a study of Cooney et al. (2015) who demonstrate that being proud to tell others about an extraordinary experience comes at a cost of fearing social rejection. Similarly, Exline and Lobel (1999) postulate that individuals are tensed between the feeling of pride and concerns about others' well-being. Hence, sharing positive information about oneself might eventually jeopardize the fundamental goal of maintaining close and secure relationships with others (Exline and Lobel 1999).

As individuals seek for social approval and strive to avoid disapproval, they worry about misperceptions others might have of them (Schlenker 1975). Specifically, they are trying to protect their social image and consciously adjust it in line with the expectations of the audience (Goffman 1975). However, while in face-to-face communication people can observe the reactions of others directly following their self-disclosure (Walther 1996), SNS users have to predict it. Thus, the challenge of presenting oneself favorably is magnified on SNS. Indeed, in a study of Lee et al. (2013) 22% of the participants were concerned about the risk of losing face on an SNS, for example by being seen as foolish. Other studies emphasize the risk of being viewed as arrogant (Berman et al. 2015) or a show-off (Krasnova and Kift 2012) on SNSs, as also evidenced by our qualitative study (Table 23). Hence, since SNS users (just as any other individuals in social contexts) seek to be seen as likeable in order to maintain a desirable social image (Leary and Kowalski 1990) and mutual relationships (Baumeister and Leary 1995), fear of being negatively evaluated by others can counteract these goals. Thus, independently of the pleasure of self-enhancing in front of others, people may fear to be negatively evaluated which impedes self-disclosure on SNS. This leads us to the following hypothesis:

H4: The fear of being negatively evaluated by others is negatively related to the intention to disclose information on an SNS.

Extension of the Privacy Calculus by a Social Calculus

Interpersonal communication research suggests that senders take the perspective of their communication partners in an attempt to evaluate how their message will be perceived and evaluated by the receiving audience in order to achieve successful communication (Galinsky et al. 2008). Given that the presence of others is an inherent element of SNS participation, we postulate that SNS users will also engage in perspective-taking when disclosing on the platform. Partly, this motivation could be rooted in users' desire to be rewarded by their audience in the form of 'likes' or other positive feedback (S. Y. Lee et al. 2016). Indeed, our qualitative pre-study has shown that users strive to share content they consider valuable for others. While the value of shared content is a multi-faceted phenomenon, a two-fold differentiation between hedonic and utilitarian dimensions has been particularly salient in marketing studies (Voss et al. 2003), SNS research (Koroleva et al. 2011; Wagner et al. 2018b), and our pre-test (see Table 23). The hedonic dimension can be best described in terms of "sensations derived from the experience" of viewing the content (e.g. beautiful landscape, nicely arranged objects) (Voss et al. 2003, p. 310), and largely reflects the aesthetic dimension of the content. At the same time, the utilitarian dimension describes the usefulness of the content for others, which is reflective of the practical relevance of the information contained in it.

Indeed, previous SNS research highlights that users tailor the content of their message with regard to their audiences' knowledge and interests (Schau and Gilly 2003; Sleeper et al. 2013). In terms of utilitarian dimension, users have been shown to refrain from sharing boring or repetitive content with their audience aiming to post relevant updates (Krasnova and Kift 2012) that do not overload their readers (Tufekci 2007). On the hedonic front, users seek to entertain themselves and others (Chennamaneni and Taneja 2015), and construct their message in the most appealing way to please their audience. For instance, users have been shown to invest effort in message construction and photo-taking in order to provide aesthetic content and inspire others (Pinkerton et al. 2017). Hence, we hypothesize that:

H5a: The anticipated hedonic value of a shared message to others is positively related to the intention to disclose information on an SNS.

H5b: The anticipated utilitarian value of a shared message to others is positively related to the intention to disclose information on an SNS.

While users may genuinely strive to deliver utilitarian and hedonic value to their audiences (Krasnova and Kift 2012; Wagner et al. 2018b), their efforts may backfire in terms of resentful reactions from others (Scopelliti et al. 2015). Indeed, a growing body of research suggests that recipients are far from being appreciative when viewing the content their friends share on SNSs. Considering that posts shared on SNSs are overwhelmingly positive in nature (Berman et al. 2015; Kim et al. 2016; Lyu 2016; Qiu et al. 2012), negative emotions of the recipients, such as envy (Krasnova et al. 2015), anger and annoyance (Fox and Moreland 2015; Peña and Brody 2014) are widespread. For example, the findings of Krasnova et al. (2015, Table 4) reveal that feelings of envy surpass any other emotion experienced by "others" on the network. Thus, disclosing positive information on SNS can cause tremendous social costs to others (Cooney et al. 2015; Exline et al. 2004). Against this background, users might find themselves in a situation where they have to balance their own benefits of self-disclosure, with interpersonal empathic concerns regarding hurting the feelings of their audience (Baumeister and Leary 1995). Hence, we presume that

sharing positive news of oneself is impeded by anticipated negative feelings of others. Therefore, we hypothesize:

H6: The anticipated negative affect of others is negatively related to the intention to disclose information on an SNS.

Being in a painful state of negative affect, recipients may eventually develop adverse perceptions towards the sender, who has caused their “suffering” (Exline et al. 2004). Indeed, psychology and organizational research consistently shows that envy may lead to such unpreferred emotion-coping behaviors as the desire to hurt (Cohen-Charash 2009) or belittle (Moran and Schweitzer 2008) the comparison target. For example, education research reveals that academically superior students fear upward comparisons towards them, as they may subsequently result in negative reactions of others (Cross et al. 1991), who may call them “nerds”. In other words, beyond experiencing negative feelings themselves, recipients may also direct this negativity towards the sender. Hence, anticipation of negative affect of others is likely to magnify the fear of being negatively evaluated by others among senders (Exline and Lobel 1999). Along these lines, we hypothesize:

H7: The anticipated negative affect of others is positively related to the fear of being negatively evaluated by others on an SNS.

Quantitative Main Study

In the following main study, we build on the results of our pre-study along with the theoretical foundation of perspective-taking (Galinsky et al. 2008; Westley and MacLean Jr 1957), and empirically test our developed hypotheses. We conducted an anonymous online survey which is common in SNS-related studies (Jia et al. 2010; Lee et al. 2014). The online survey commenced with a welcome page briefly describing the goal of the study (investigating sharing decisions on SNS) and guaranteed full anonymity of respondents’ answers. Furthermore, the dependent variable was measured before the independent variables and the function to move backwards to prior survey pages was disabled to prevent participants from changing answers retrospectively. All of these remedies helped us to mitigate the risk of common method bias (Podsakoff et al. 2003).

With the assistance of a market research firm, we distributed the survey link to Facebook users. Collecting data this way has helped us to target an anonymous panel of respondents who are active on Facebook and willing to participate in research studies. Facebook was chosen as the research case, because it is the leading SNS platform (Statista 2017b), and users are routinely sharing vast amount of information on the network. We have opted for a scenario-based research design, which is common in marketing studies (Barasch and Berger 2014; Berman et al. 2015), and was also widely applied in the SNS context (Oh and Larose 2016). Specifically, respondents were presented with a hypothetical scenario in which they were asked to imagine that they were on vacation at a beautiful beach resort. In the next step, respondents were shown a photo, presented as a Facebook post, which they have allegedly taken during this vacation. The photo showed a beautiful scenery of the beach with a palm and a small footbridge into the sea. This picture was chosen based on a small pre-test among 152 students in comparison with other three vacation pictures (including a picture of a cocktail at the beach, a fancy hotel room, and a skiing picture). It scored highest in terms of being commonly shared and seen on Facebook, self-relevance (the likelihood that the picture could have been taken if one would have had such vacation), and visual appeal. Overall, our choice of the scenario-based approach has helped us to control for the type of travel experience across all survey participants.

All measurement scales have been based on prior literature and measured on a 7-point Likert scale ranging from ‘strongly disagree’ to ‘strongly agree’ except for the construct “intention to self-disclose”. This scale (INT) was adopted from Malhotra et al. (2004), and was formulated as follows: “What do you think: Would you share this photo of your holiday experience?”, and measured with the help of a 7-point semantic differential anchored with unlikely/likely, not probable/probable, impossible/possible, unwilling/willing. To measure the anticipated value of a message for others, we relied on a scale often used in marketing literature to capture customers’ attitude towards a product (Voss et al. 2003). It distinguishes the utilitarian (UTIL) and the hedonic (HED) dimension with three items each: “relevant”, “useful”, “interesting”, as well as “appealing”, “nice”, and “engaging” respectively. To capture anticipated negative affect of others (NAF), we relied on two sources. Specifically, we took three “negative affect” items from the PANAS-X scale (Watson and Clark 1999) in order to comprehensively capture individual concerns about others’ feelings: “Sharing this post on Facebook, I am concerned that others could be ...” (1) upset, because such vacation is currently not feasible for them, (2) annoyed that I share such a photo, (3) sad because they cannot experience such a vacation right now”. Additionally, we added two items from the envy scale from Krasnova et al. (2015), since envy was the predominant negative feeling mentioned in our qualitative pre-study: “Sharing this post on Facebook: ...” (1) “I am concerned that others might think I am having a better life than they have”, (2) “I am concerned that others feel worse compared to me”.

Fear of being negatively perceived (FNP) by others was measured with items adapted from Lee et al. (2013) (who refer to it as “face risks”), and Berman et al. (2015) (who refer to it as “self-presentational concerns”): “When sharing this photo on Facebook, I would be concerned that others...” (1) would perceive me as a show-off, (2) would see me as arrogant, (3) would consider me as insincere, (4) might misunderstand me”. For convenience of relationship maintenance (REL), we relied on a scale from Krasnova et al. (2010a) measuring the extent to which sharing content is an efficient form of communication: “Sharing this photo on Facebook would help me to... (1) stay in touch with others, (2) maintain friendships, (3) keep others up-to-date, (4) communicate with others about my life, (5) inform others about me”. Self-enhancement (ENH) was measured based on the scales of Krasnova et al. (2015; 2017; 2010a), which were slightly modified to reflect the feelings of private pleasure and pride mentioned in the pre-test. Items were formulated as follows: “(1) It would feel good to show everyone what I have experienced, (2) It would make me proud to tell others about my travel experience, (3) It would feel good to show everyone how beautiful my trip was, (4) It would make me proud to show everyone where I went on vacation, (5) It would make me happy to show my holiday experience to others”. Privacy concerns (PC) were measured on the basis of an “organizational privacy concerns” scale by Krasnova et al. (2009a), which is frequently applied in the SNS context: “Sharing this post, I would be concerned that it: (1) ...can be used for commercial purposes (e.g., personalized advertising), (2) ...can be shared with other third-parties (e.g., advertisers, employer, state), (3) ...can be collected and stored by Facebook, (4) ...can be used to display personalized advertising to me”. Apart from the main constructs, we also captured demographics (age, gender) and frequency of posting on Facebook (ranging from ‘daily’ to ‘monthly’), as controls.

Results

A total of 263 respondents from Germany took part in the survey. To ensure high quality of our data and to identify participants who did not carefully read all items, we included an attention check into our survey (Meade and Craig 2012) Specifically, one item was added into the battery

of items measured on a 7-point Likert scale that asked participants to simply “check ‘strongly agree’”. After eliminating all participants who failed to do so (32), we were left with a net sample of 231 observations for further analysis. 135 (58.4%) of them were female and the age ranged from 18 to 35 with a mean of 28.5. The majority were employed (144), followed by students (48).

First, the quality of our measurement model was evaluated by assessing convergent and discriminant validity (Hair et al. 2013). Convergent validity describes the degree to which items within one scale are in fact statistically similar and thus measure the intended construct. It is assessed by evaluating the criteria of item reliability, composite reliability (CR), the average variance extracted (AVE) and Cronbach’s α (CA) of the constructs involved. Item reliability is given when all items have loadings higher than 0.7 (Hair et al. 2013). This criterion is met for all our constructs in our model. CR is also fulfilled as it exceeds the threshold value of 0.7 across all constructs (Bagozzi and Yi 2012). Further, the AVE is higher than 0.5 for all constructs (Hair et al. 2011). Cronbach’s α also exceeds the threshold of 0.7 for all constructs involved (Bagozzi and Yi 2012). To conclude, all criteria for convergent validity are met (see Table 24). Discriminant validity was assessed by ensuring that the square root of AVE for each construct was higher than the correlation between this construct and any other construct in the model (Fornell and Larcker 1981). This requirement was fulfilled for all constructs in our model (see Table 24). Cross-loadings were not a concern.

Table 24. Construct validity measures.

	CA	CR	AVE	FNP	HED	INT	NAF	PC	ENH	REL	UTIL
FNP	.946	.956	.844	.937							
HED	.880	.926	.807	-.386	.899						
INT	.838	.903	.756	-.407	.531	.935					
NAF	.841	.886	.608	0.430	-.111	-.135	.825				
PC	.952	.965	.874	0.311	-.094	-.083	.226	.918			
ENH	.887	.914	.680	-.212	.508	.668	.000	-.148	.935		
REL	.954	.966	.878	-.061	.551	.560	-.024	-.060	.646	.780	
UTIL	.952	.965	.875	-.199	.574	.498	-.090	.007	.467	.505	.870

Taken together, our measurement model was well-specified. In the next step, structural model was assessed. Our model explains 58.1% of variance in the dependent variable “intention to self-disclose” and 18.5% in the construct “fear of negative evaluation by others”.

Our research model was evaluated using the Partial Least Squares (PLS) approach to Structural Equation Modeling with the help of the SmartPLS 3.0 software (Ringle et al. 2015). To investigate our model relationships, a bootstrapping with 5,000 iterations was employed (Davison and Hinkley 1997). All hypothesized relationships were in the predicted direction and were significant, except for H1, H5a and H6, as outlined in Figure 12. First, for H1, it was predicted that “privacy concerns” would be negatively associated with users’ “intention to self-disclose”. However, the results did not support the presence of this relationship ($\beta = -0.085$, $p = 0.122$). Second, the “anticipated hedonic value” of the message for others was not significantly related to “intention to disclose” ($\beta = -0.010$, $p = 0.613$) in our model. Third, for H6, it was postulated that “anticipated negative affect of others” would negatively influence “intention to self-disclose”. This link also turned out to be insignificant ($\beta = 0.033$, $p = 0.841$). Interestingly, none of the control variables we tested - age, gender, and posting frequency - turned out to be significant.

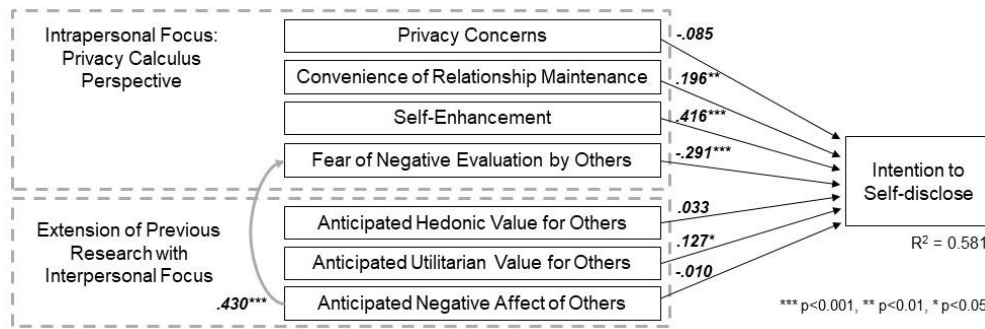


Figure 12. Research model with path coefficients and significance levels.

Importantly, however, our ad hoc analysis has revealed that “fear of negative evaluation by others” fully mediates the relationship between “anticipated negative affect of others” and “intention to self-disclose”, which has significant implications in terms of our findings. Following Baron and Kenny (1986), full mediation takes place when a significant path in a direct model becomes insignificant once the mediator variable is added. A full mediation assumes that relationships between an independent variable (“anticipated negative affect of others”) and the mediator as well as the dependent variable (“intent to self-disclose”) are significant, which is the case for our model. The removal of “fear of negative evaluation by others” construct revealed a significant negative path between “anticipated negative affect of others” and “intent to self-disclose” ($\beta = -0.132$, $p = 0.048$). The Sobel Test statistic used to test the mediation effect in a mediated model was also significant ($p = 0.000$).

Discussion

The goal of our research was to uncover mental processes behind self-disclosure decisions on SNSs. Specifically, we questioned whether senders care about subsequent perceptions and emotions of others when communicating on SNS and to what extent these perceptions influence self-disclosure decisions. Building on interpersonal communication theory in general (e.g., Berlo 1960) and perspective-taking literature in particular (e.g., Van Boven and Loewenstein 2005), we provide empirical evidence for our propositions based on a qualitative pre-study and a main quantitative study with 207 and 231 Facebook users respectively. Hereby, we add to existing theory in several ways.

First, we show that SNS users are tensed between their desire to experience private pleasure of self-enhancement and their fear of being negatively evaluated by others. While self-disclosure can be privately pleasurable, users may still refrain from sharing if they feel that their social image is in danger. Hereby, we incorporate the fear of being negatively evaluated into the intrapersonal calculus and provide evidence of Forster’s competitive and fear axis in the SNS context (Foster 1972). We underpin the vital motive of self-presenting oneself in the best light possible while navigating impression on others on SNSs (e.g., Mehdizadeh 2010).

Interestingly, our results did not find evidence for the negative link between privacy concerns and intention to self-disclose, predominantly assumed in SNS research. This finding stays in contrast to established SNS research built on the privacy calculus model (e.g., Cheung et al. 2015; Krasnova et al. 2010a). Considering that data collection was conducted amidst the recent Facebook-Cambridge Analytica scandal that took place in March 2018, these findings are particularly surprising. However, research argues that SNS users have lower privacy risk perceptions as compared to non-users and therefore they are less concerned about the misuse of their personal

information (Fogel and Nehmad 2009). Furthermore, research based on the elaboration likelihood model (Petty and Cacioppo 1986) assumes that privacy concerns are only relevant when individuals are able and motivated to process it which requires careful thoughts (e.g., Lowry et al. 2012). Thus, individuals who have low expertise in the privacy field or who are unwilling to invest cognitive resources will only passively process information on privacy concerns and thus are less likely to consider them in their decision-making. Against this background, we conclude that SNS users do not engage in central processing (cognitive effort) when it comes to privacy, but central processing is applied to social concerns. Based on our results, we challenge the critical role of privacy concerns as impediment of self-disclosures on SNSs. Users seem to be more concerned about threats to their social image as opposed to the misuse of information by organizations.

Second, we extend the intrapersonal privacy calculus by interpersonal determinants of self-disclosure. Specifically, we identified three interpersonal antecedents in our qualitative pre-study: anticipated negative affect of others, and anticipated utilitarian and hedonic value of the shared message for others. By incorporating social concerns into the privacy calculus, we move beyond the narrow fear of misuse of personal information established in the e-commerce environment where communication takes place between a user and a single provider (Dinev and Hart 2006). Because on SNS communication is inherently social with individuals sharing their self-presentational content (Min 2016), we were able to show that SNS users think about other's feelings when deciding to disclose a message. However, this effect was mediated by their fear of being negatively perceived by others. In this light, we contribute to the scientific discussion whether virtual communication leads to less empathy among its users (Alloway et al. 2014). An examination of American college students between 1979 and 2009 found that with the introduction of SNS empathic concerns and perspective-taking levels decreased (Konrath et al. 2010). Carrier et al. (2015) explains this fact by a lower degree of social cues in online communication as is apparent in face-to-face communication. However, our results suggest that SNS users are concerned about others' feelings as it may backfire to the way how they are perceived and evaluated by others.

Surprisingly, the anticipated hedonic value of the shared message for others turned out to be insignificantly related to self-disclosure, while the anticipated utilitarian value plays an essential role. Against the background of interpersonal communication theory highlighting the importance of usefulness of a message, and the well-known slogan "content is king", we deem this result to be justifiable.

Additionally, our results also offer practical implications for SNS providers and users. SNS providers can help users to construct their messages in accordance with the needs and interest of the audience. They can reference prior messages which were very successful in terms of positive feedback from the audience to guide future message construction. In this vein, they can leverage the quality of the user-generated content on their platform in order to counteract needless and annoying information. As user-generated content is the backbone of each SNS platform, relevant information for recipients can drive user satisfaction and thus loyalty (Wagner et al. 2018b). On the negative side, message contribution is impeded by the fear of being negatively evaluated. Research has shown that these risk perceptions can be mitigated by self-presenting oneself more modest (Scott and Ravenscroft 2017). To enhance sharing, SNS providers can offer functionalities which simplify this self-presentation style, for instance by designing more authentic and natural filters or photo-editing tools. For users, our results shed light on the tension between own benefits and risks and others' benefits and risks. Users are indeed aware that their shared content is perceived, evaluated and judged which might contribute to successful communication for both

parties or backfire in terms of negative evaluation. They weigh up their own tradeoff against the tradeoff for others and subsequently decide whether sharing a message will be beneficial for both communication partners. To conclude, while SNS communication suffers from less social cues, it is still a marketplace for social communication and thus perspective taking needs to be taken into account when examining users' antecedents of self-disclosure on SNS.

Limitations and Future Research Suggestions

Certainly, our study is not free from limitations. First, we relied on a panel of a market research firm. Even though this is common in IS research, we gathered data from respondents who are willing to participate in a survey for a relative small incentive. However, it helped us to target anonymous Facebook users instead of a convenient student sample. Against the background of commonly shared messages on SNS, we decided to focus on positive self-expressive messages. This decision was grounded in the assumption, that the overwhelming amount of shared messages is positive with people displaying their accomplishments and good deeds. Despite our results, future research can test whether perspective-taking is also present when revealing negative or support-seeking messages. Moreover, we tested our hypotheses based on stated intentional behavior with regard to one vacation picture. Although, we selected the hypothetical scenario carefully, our findings need to be validated in a more realistic manner measuring actual behavior. Our results also offer suggestions for future research projects. We found evidence that SNS users engage in perspective-taking when deciding to share a message. However, it remains unclear whether the magnitude of perspective-takings varies depending on the network size and structure of each user. We could imagine that the level of perspective-taking is higher when individuals are communicating to a network consisting of close friends compared to distant acquaintances.

Conclusion

Every social communication starts with social thoughts. Thus, self-disclosure decisions in a social marketplace like SNSs indeed involve interpersonal concerns. Individuals step into the shoes of others in order to evaluate how others feel and in turn perceive them. Moreover, they anticipate the relevance of their message for their audience. Thus, they are less egoistic as typically assumed by the privacy calculus model guided by an intrapersonal tradeoff between own benefits and privacy concerns. They are tensed between their pleasure of self-enhancing in front of their audience and others' distress caused by their own behavior. However, although users think about others when sharing, their concerns are also self-focused as others' emotional harm can backfire to their social image.

10 Research Paper 3.C: Perspective-taking Bias on SNS

Title: When You Share You Should Care: Examining the Role of Perspective-taking on Social Networking Sites

Authors: Wagner, Amina; Abramova, Olga; Krasnova, Hanna; Buxmann, Peter

Published in: European Conference on Information Systems (ECIS), Portsmouth, UK, 2018

Abstract

Despite good intentions of users who share updates on SNSs, there is mounting evidence that recipients of SNS content frequently perceive shared information as inappropriate, annoying, envy-inducing, and excessive. To examine this apparent gap, we draw on the communication theory and the perceptual congruence model to analyze perceptual differences with the help of dyadic data analysis. Our findings based on 90 sender-recipient pairs show significant perceptual differences between senders and corresponding recipients of content, with senders attaching greater value to their content and scoring both hedonic and utilitarian attributes higher. Additionally, we demonstrate the presence of “false consensus effect” in the SNS environment, meaning that senders anticipate perceptions of recipients to be more similar to their own, than they actually are. Our results provide evidence that sender’s accuracy in predicting recipient’s perceptions contributes to favorable outcomes for both parties, including recipient’s satisfaction with the SNS relationship and positive feedback, desirable for senders. This highlights the importance of perspective-taking ability among senders of content. Implications for stakeholders in research and practice are discussed.

Keywords: Social Networking Sites, Perspective-Taking, Perceptual Congruence Model, Audience Awareness, Dyadic Study

Introduction

In today's digital world, Social Networking Sites (SNS) are the marketplace where social interaction takes place. SNS users interact with each other by contributing and consuming user-generated content (Zeng and Wei 2013), taking on sender and recipient roles respectively. Every minute 293,000 statuses are updated and 136,000 photos are uploaded (Zephora 2015) by senders on Facebook and immediately seen by recipients who browse others' activities and content through the aggregated stream of news ("News Feed") (Burke et al. 2010).

Senders claim to carefully craft their own shared content (Sleeper et al. 2013), aiming to contribute to relationship maintenance (Chennamaneni and Taneja 2015; Krasnova et al. 2010; Maksl and Young 2013) and building (Krasnova et al. 2017), share relevant news (Krasnova and Kift 2012) as well as entertain themselves and others (Chennamaneni and Taneja 2015; Cheung et al. 2015; Kim et al. 2015; Utz 2015). Thereby, they seek to leave favorable impressions (Krämer and Winter 2008; Walther 2007). Research evidences that senders of content get intrinsically rewarded by a feeling of social connectedness (Utz 2015) and extrinsically through the positive feedback in the form of 'likes' (Lee et al. 2016).

Despite these good intentions pursued by information senders, growing scientific evidence reports alarming experiences of recipients caused by the amount and type of content shared on the network, including information overload (Lee et al. 2016; Sasaki et al. 2016) and the need to manage inappropriate as well as annoying content (Fox and Moreland 2015; Peña and Brody 2014). Recent survey among adults in South Korea has shown that 69.4% are tired of their SNS, specifying needless information (27.7%) as the main reason (Korea Bizwire 2017). Among other undesirable consequences of content consumption by recipients are feelings of envy (Krasnova et al. 2015; Tandoc et al. 2015), negative moods (Sagioglou and Greitemeyer 2014) and a decline in well-being and life satisfaction (Burke et al. 2010; Frison and Eggermont 2016). Altogether, it appears that ongoing SNS communication lacks efficiency: while senders are trying their best to leave good impressions, recipients do not seem to pick up on these intentions.

Drawing on the interpersonal communication theory and perceptual congruence model (Acitelli et al. 1993; White 1985), we argue that perceptual differences between communication parties coupled with the poor ability for perspective-taking account for the observed "sender-recipient" contradictions. Defined as one's ability to see things from another person's viewpoint (Galinsky et al. 2008), the importance of perspective-taking has been shown across a variety of communication contexts including business-IT alignment (Benlian and Haffke 2015), romantic relationships (Acitelli et al. 1993) as well as parent-children relationships (Fingerman 1995). Building on the results of the social and personal relationship research stream, this paper focuses on the role of perspective-taking as an overlooked aspect of SNS communication.

We started from the premise that technology-related properties of the SNS communication such as reduced number of available social cues (Walther 1996), heterogeneous audience (Acquisiti and Gross 2006) and asynchronicity in the communication loop, challenges efficient communication in accordance with sender's goals and recipient's interests. Against this background, we argue that *perspective-taking* can be used to *explain* communication misperceptions which lead to negative effects on the recipient side. Methodologically, our study extends past SNS research which has mainly followed a one-sided approach examining either the determinants of content-sharing from sender's perspective (Hollenbaugh and Ferris 2014; Krasnova et al. 2010a) or the outcomes of content consumption from recipient's perspective (Burke et al. 2010; Krasnova et al. 2015). We accentuate that communication involves at least two

parties and success of social interaction in many ways is influenced by, if not dependent, on interpersonal processes. Based on a two-sided design, relying on dyadic data analysis, our study addresses the following research questions:

Do information senders and recipients perceive shared content differently on SNSs?

Are senders egocentric when predicting perceptions of recipients with regard to the shared content?

How does perspective-taking ability of the sender affect recipient's satisfaction with the online relationship and further his or her content-related actions?

Disentangling intra- and interpersonal effects on the communicational outcomes, this paper makes several timely and scholarly contributions. First, significant perceptual differences between senders of the information and corresponding recipients are demonstrated, with senders attaching higher value to both hedonic and utilitarian attributes of the self-generated content. This supports the proposition that on SNS active usage of sharing functionalities is more beneficial than the passive consumption (Krasnova et al. 2015; Wenninger et al. 2016). Second, "false consensus effect" is confirmed meaning sender's delusion and overestimation of the actual opinion similarity with the recipient. Next, according to our theoretical model, the dyadic data analysis asserts the link between sender's ability for perspective-taking and important relational outcomes such as recipient's satisfaction with the online relationship, feedback valence and the intention to hide or ignore the content. For senders, these findings tip off that egocentric content-sharing can backfire on them when recipients provide less positive feedback and in the worst case stop consuming future content. For SNS providers, our results hint at the possibility to introduce more sophisticated feedback *mechanism* and News Feed *filtering mechanism* to keep the feed relevant for the readers while sensitizing senders that messages need to be constructed in accordance with their recipients' needs.

Conceptual Background and Hypotheses Development

In this section, we build on the interpersonal communication theory (Berlo 1960; Westley and MacLean Jr 1957) in order to describe how social interaction takes place on SNS. Thereby, we provide arguments why the concept of perceptual congruence (White 1985) and the underlying need for perspective-taking (Epley et al. 2004; Ross et al. 1977) in interpersonal communication is necessary. Based on this, we derive our hypotheses and formulate a theoretical model.

To describe the relationships between users on SNS, we adopt the "sender-recipient" model (Figure 13), originally proposed by Westley and MacLean Jr (1957) and later extended by (Berlo 1960). In general, it is assumed that a sender has an idea or content which he or she would like to share with a recipient through a certain medium. When the message has been received, the recipient can react on it and potentially provide feedback for the sender, thus closing the loop and making a single communication complete. In order to achieve efficient communication and thus a satisfying relationship, the recipient has to pick-up the idea of the sender. In other words, the message has to be understood by a recipient in a way anticipated by the sender (Westley and MacLean Jr 1957).

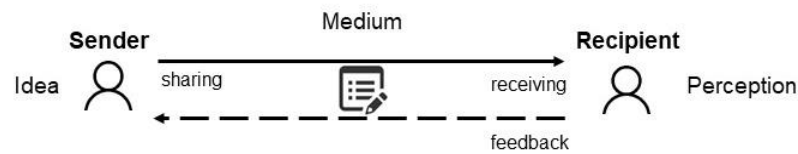


Figure 13. Sender-recipient relationship on SNSs.

In contrast to face-to-face interactions, technology-related properties of SNSs as a medium metamorphose the communication. As such, the limited number of social cues (e.g., unawareness of appearance, gestures or facial expression) and asynchronicity (communication with time lag) (Walther 1996) shifts the focus from the form (i.e. how a message is broadcasted) to the subject (i.e. what is broadcasted) and thus making the “*content is king*” claim (Gates 1996) especially relevant in the SNS environment.

Established SNS literature relying on the privacy calculus model (Culnan and Armstrong 1999; Dinev and Hart 2006) proposes that when making a decision whether to share a content, a sender as a creator and an initial owner of the content weighs potential benefits and costs of content disclosure (Krasnova et al. 2010a). When the benefits of disclosure (e.g., relational benefits, enjoyment, need for self-presentation) outweigh the risks (e.g., privacy or audience concerns), users will publish the content online (Cheung et al. 2015; Krasnova et al. 2010a). Hence, for the already published content it has been decided that benefits are higher than costs. Therefore we expect that the sender’s valuation of the own content is relatively high. This assumption is supported by the concept of effort in marketing asserting that greater effort increases the perceived importance of the product (Cardozo 1965). In line with it, past research evidenced careful selection and content crafting among SNS users (Lyu 2016; Marwick and Boyd 2011; Sleeper et al. 2013). Examination of 3.9 million Facebook users revealed self-censorship in 71% of cases (Das and Kramer 2005) which hints at high diligence from the sender side and consequently significant appraisal of the own shared message.

Recipient as a consumer of content can form an attitude (Voss et al. 2003) towards the seen content and provide feedback. Based on Voss et al. (2003) we adopt a two-dimensional conceptualization of consumer attitudes differentiating between utilitarian and hedonic values. While utilitarian benefits refer to the informative character and relevance of the shared content, hedonic value reflects its appealing and enjoyable nature (Brakemeier et al. 2016b; Voss et al. 2003). In contrast to a purchase, on SNS recipients get the published content pushed through the News Feed and are thus exposed to forced content consumption. As such, not all items in the News Feed may be relevant and enjoyable to the recipients which decreases the subjective average value of the information received. Indeed, research demonstrate that there is a gap between the content that is liked to be shared and the content that is liked to be read on SNS (Gong et al. 2016). Therefore, we hypothesize:

H1a: On SNSs, sender’s perception of the hedonic value of the content is higher than the recipient’s perception of the hedonic value of the content on SNSs.

H1b: On SNSs, sender’s perception of the utilitarian value of the content is higher than the recipient’s perception of the utilitarian value of the content on SNSs.

Perceptual Congruence and Perspective-taking

Originally stemming from social cognition theory (Bandura 1986), perceptual congruence model describes the fit between two perceptions of the same social stimulus (Srull and Wyer 1988). Social cognition theory has been widely used in communication research in order to study how

communicators behave and learn in social interactions (Bandura 2002). According to this approach, individuals initially evaluate their own perception of the stimulus (the shared content in the SNS context) and then subsequently anticipate how others might perceive it (Epley et al. 2004). High perceptual congruence implies a high degree of alignment within social connections, whereas low congruence signifies perceptual differences. To achieve congruence, perspective-taking should take place, which involves examining perceptions of the stimulus from the viewpoint of another person (Ross 1977). This process is referred to as the ability to relate to others. As such, perspective-taking has been recognized as an important precondition to successful social communication (Epley et al. 2004; Schlenker and Leary 1982, Dunning et al. 2001). Indeed, assessing perspectives of others adequately leads to greater understanding in interpersonal communication and thus effective relationship management (Morrison and Bellack 1981). For example, importance of perspective-taking has been exemplified in studies between husbands and wives, demonstrating that a common understanding of each other drives marriage satisfaction (Acitelli et al. 1993; Schröder-Abé and Schütz 2011). At the same time, insufficient perspective-taking has been linked to enmity (Dunning et al. 2001), misunderstanding (Kruger et al. 2005) and a lower level of team performance (Benlian 2014).

The perceptual congruence model suggests three measures to study relationships, differentiating between interpersonal and intrapersonal parameters (White 1985), as described in Table 25.

Table 25. Explanation of perceptual congruence measures (S- Sender; R- Recipient).

Perceptual Congruence Measures	Explanation (adapted from White 1985)	Examples from our study
Actual Agreement	Congruence of the reported actual perceptions of senders and recipients [interpersonal].	S: "I find my post ...interesting" R: "I find the post of my friend (S) ...interesting"
Perceived Agreement	Congruence of the sender's reported perception and sender's anticipation of recipient's attitude/perception [intrapersonal].	S: "I find my post ...interesting" S: "My friend (R) finds my post ...interesting"
Sender's Understanding of the Recipient (also: Interpersonal Understanding)	Congruence of the sender's anticipation of recipient's attitude/perception and the recipient's actual attitude/perception [interpersonal].	S: "My friend (R) finds my post ...interesting" R: "I find the post of my friend ...interesting"

Agreement between senders and recipients on SNS

Applying the perceptual congruence model to SNS communication, we examine the individual attitudes of both members of a dyadic "sender-recipient" pair and sender's anticipation of recipient's opinion as depicted in Figure 14. Comparing sender's opinion on the shared content with the recipient's opinion allows to assess the degree of actual congruence (Figure 14: '1-actual agreement'). The second measure, perceived agreement, compares the sender's assessment of the content with the sender's prediction of recipient's opinion. As such, it reveals how strongly senders believe the recipients have the same viewpoint on the posted content (Figure 14: '2-perceived agreement'). The third parameter, interpersonal understanding, contrasts sender's anticipation of recipient's assessment with the recipient's actual assessment, thus indicating sender's prediction accuracy (Figure 14: '3-sender's understanding of recipient'). Although originally perceptual congruence model is built around the concept of parity between partners

and promotes the importance of mutual understanding (Acitelli et al. 1993), in our study perspective-taking ability of the senders are given a priority, as to the party empowered to commence the virtual conversation.

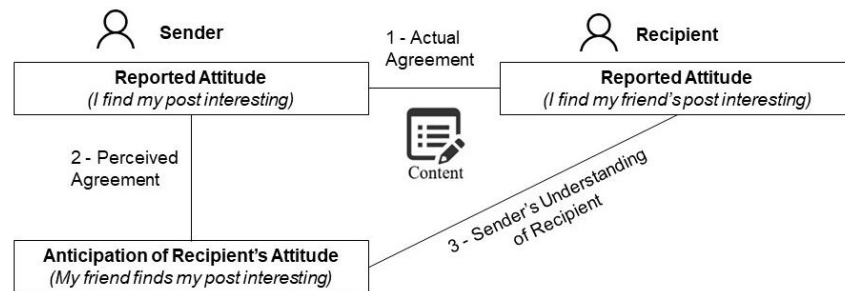


Figure 14. Perceptual congruence model of the shared content value.

Starting with perceived agreement (Figure 14 – left two boxes), extant research suggests, individuals use their own perceptions ('reported attitude') as an anchor to predict perceptions of others ('anticipation of recipient's attitude'). Since people tend to perceive others as being more similar than they actually are (Epley et al. 2004), the process of anticipating others' perception is assumed to be egocentric in nature. For example, studies among married couples have found empirical evidence that husbands and wives perceive each other as being similar and thus more aligned on their life plans than they actually are (Schröder-Abé and Schütz 2011). Even when perceptions of others are considered, individuals seem to be inclined towards their own perception, which is referred to as the false-consensus bias (Ross et al. 1977). Compared to offline interactions, the severity of false-consensus bias may be even more accentuated on SNSs. In fact, a study of Barasch and Berger (2014) has shown that on SNS senders seem to be self-focused while being unable to fully assess the needs of their audience. Senders may increasingly choose to rely on their own interests (Barasch and Berger 2014). This, in turn, gives rise to overestimate the closeness of another's attitude to one's own perception. Since the perceived agreement is biased in the direction of oneself, we expect it to be higher than the actual agreement. We hypothesize the following:

H2a: On SNSs, sender's perceived agreement regarding the hedonic value of the content is higher than the actual agreement regarding the hedonic value of the content.

H2b: On SNSs, sender's perceived agreement regarding the utilitarian value of the content is higher than the actual agreement regarding the utilitarian value of the content.

Effects of sender's understanding on recipient's satisfaction and online behavior

In the next step, we move beyond the investigation of perceptual differences between senders and recipients towards examining consequences of (dis-)congruence between the sender's anticipation of the recipient's perception and the actual recipient's perception – a fact we refer to as the degree of interpersonal understanding (Figure 14: '3-sender's understanding of recipient').

In offline settings, a higher degree of interpersonal understanding has been linked to such positive relational outcomes as perceived collaboration quality (Benlian and Haffke 2015), marital satisfaction (Levinger and Breedlove 1966; Schröder-Abé and Schütz 2011), as well as improved team or employee performance (Benlian 2014; Evans et al. 2003; Parker et al. 2017). Allen and Thompson (1984) find a direct association between wives' understanding and husbands' satisfaction with the relationship. On SNS, a vital motive to share content is to stay connected with friends and thus building healthy relationships (for review see Abramova et al. 2017). The sender as the generator of shared content is supposed to understand the recipient in order to obtain

relationship satisfaction indicated by the recipient. Clearly, the more accurate the senders predict the perception of their audience, the more likely they are to share information which corresponds to the needs of the recipients and in turn contribute to recipient's satisfaction with the online relationships. Based on this line of reasoning, we hypothesize that:

H3a: On SNSs, the degree of sender's interpersonal understanding of the hedonic value of the content is positively associated with recipient's satisfaction with the online relationship.

H3b: On SNSs, the degree of sender's interpersonal understanding of the utilitarian value of the content is positively associated with recipient's satisfaction with the online relationship.

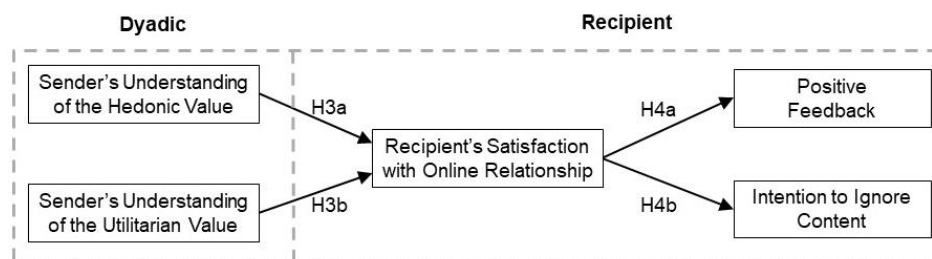


Figure 15. Research model on the effects of sender's understanding of the recipient.

Finally, to illustrate far-reaching implications of perceptual (dis-)congruence, we hypothesize that recipient's satisfaction with the online relationship with the sender impacts his or her behavioral outcomes directed to the content. Connecting recipient's satisfaction to behavioral implications is necessary since it highlights the criticality of the communication loop between sender's input (the shared content) and recipient's interpretation and reaction. Against the background of previous work (Christofides et al. 2012; Lee et al. 2016; Peña and Brody 2014), we differentiate between two proactive strategies a recipient can apply to the content displayed in the News Feed. First, when the recipient is satisfied with the content and thus with the relationship, he or she may choose to provide positive feedback by clicking on 'Like' as a form of overt approving (Pinkerton et al. 2017). By following this strategy recipients please senders and foster the mutual relationship (Lee et al. 2016). Second, as there is no 'dislike'-button available on dominant SNS platforms, when dissatisfied with the relationship, recipients may follow a neglecting strategy. Building on the established link between dissatisfaction and intentions to damage or terminate the relationship (Turel 2015), we argue that the recipient may choose to stop consuming the content of the sender. For instance, SNS provide functionalities to hide content to avoid getting to see future content from this sender, or recipients may simply proactively ignore the content from this sender when going through the News Feed. Indeed, Peña and Brody (2014) demonstrate that a relationship damage due to inappropriate content shared by others leads to recipient's intention to hide future content from this specific SNS connection. In line with these two proactive strategies, we hypothesize that:

H4a: On SNSs, recipient's satisfaction with the online relationship is positively associated with the positive feedback in the form of 'likes'.

H4b: On SNSs, recipient's satisfaction with the online relationship is negatively associated with recipient's intention to ignore the content of the sender in their News Feed.

Research Method

To validate the proposed hypotheses, a dyadic survey has been designed and pre-tested by two researchers to check for understandability of the questions. The two surveys were then

implemented in the form of an online questionnaire - one for the sender and another one for the recipient. Participants were compensated with a €10 Amazon gift card for their participation. To avoid priming, participants were told that the study aimed at understanding user behavior on SNSs. Furthermore, we assured the participants that their answers will be treated anonymously and that there were neither wrong nor false answers, so they can answer all questions honestly. Thereby, we counteracted common method (Podsakoff et al. 2003) and social desirability biases (Reynolds 1982).

Procedure and Sample

Users of the two most popular SNSs, Facebook and Instagram (Statista 2017b), were contacted with the offer to participate in the survey. To get dyadic data, participants were asked to randomly list up to three people (also referred to as network friends) from their contact list on SNS who probably would also like to participate in a survey. Once a proposed candidate has agreed, a pair (dyad) was formed. We assigned the first contacted person to the “sender” condition and the one who was suggested – to the “recipient” condition.

Before commencing with the online questionnaire, we first asked the sender to provide their most recent shared content in their own SNS account. Thereby, our study focuses on the contribution and consumption of user generated content on SNS typically expressed via self-expressive posts about thoughts or experiences (Burke et al. 2010). Thus, the following exclusion criteria were applied: (1) re-shared links, events and news, (2) re-shared information about the self initially published by another person; (3) re-shared photos copied from a third-party source. After that, the sender and the recipient received a link to the online survey, where they had to answer survey questions with regard to this specific post. The name of the corresponding dyadic partner was revealed to ensure each participant was thinking about a certain SNS connection while answering the questions. We used a unique identification number to match the dyads and to ensure anonymity within the dataset. A screenshot of the focal post was also sent by the sender to the team of researchers. In doing so, we were able to send it to the corresponding recipient in order to ensure that the recipient is answering all questions related to the exact same post.

A total of 189 responses were collected. Among them 9 responses came back without a matching partner and, hence, were removed from the dataset. The final set of 90 dyads (37 from Instagram and 53 from Facebook users) served as a basis for further analysis.

Measurement

Before testing our hypotheses we first continue with the presentation of measurements along with its validity testing to ensure convergent and discriminant validity of the applied measures.

The sender and the recipient treatment in the survey contained the same construct items to assess the hedonic and utilitarian value of the shared content, measured on a 7-point Likert scale (1=strongly disagree; 7=strongly agree). Following Wittenberg et al. (2014) and Voss et al. (2003), the scale items for reported attitude of the sender and the recipient equally (see Figure 14 and 15) included: “*I find this post “enjoyable”, “appealing”, “amusing”* to measure hedonic and “*informative”, “relevant”, “interesting”* to measure utilitarian value of the shared content. Reliability analysis based on inter-item correlations and Cronbach’s alpha (CA) (Hair et al. 2014) revealed low values of inter-item correlations for the item “*amusing*” within the hedonic dimension. This is not surprising since the majority of posts in our sample were not particularly entertaining (e.g., $\text{mean}_{\text{amusingS}}=4.29$; $\text{mean}_{\text{amusingR}}=3.69$), but otherwise could be characterized as “*enjoyable*” or “*appealing*” (see Figure 17). Therefore, this item was dropped from the hedonic

scale. Resulting CA values across scales were acceptable: $CA_{\text{hedonic}}=0.791$; $CA_{\text{utilitarian}}=0.766$ for senders; and $CA_{\text{hedonic}}=0.849$; $CA_{\text{utilitarian}}=0.840$ for recipients. Additionally, we measured sender's *anticipation of recipient's attitude* (see Figure 14), which was captured as "Think of your Facebook/Instagram friend (a matched recipient from the dyad). He/she will find this post..." while keeping the same scale items for the hedonic and utilitarian value as specified above. Internal consistency of the scale was acceptable with $CA=0.834$ for hedonic and $CA=0.790$ for utilitarian dimensions.

To compute interpersonal and intrapersonal congruence measures (Figure 14, Table 25) we followed the approach of Acitelli et al. (1993), which was introduced to the IS literature by Benlian and Haffke (2015). Rather than using the absolute difference of two dyadic responses, this technique assigns a congruence score (CS) between 1 (complete incongruence) and 10 (complete congruence) to the pair of answers (measured on 7-point Likert scale) and takes into consideration the side of the scale spectrum (either above or under 4). For example, for responses that both fall on the same side of the answer spectrum (e.g., 5-slightly agree and 7-strongly agree; $CS=7$) relatively high congruence scores are awarded (which signifies high degree of understanding); for cases when two responses fall on the opposite sides of the answer spectrum (e.g., 3-slightly disagree and 5-slightly agree; $CS=5$), relatively low congruence scores are assigned, despite the fact that both pairs of scores have exactly two points differences. Using perceptual congruence scoring table as a basis (Benlian and Haffke 2015), (1) 'actual agreement' was derived by comparing reported attitude of the sender vs. reported attitude of the recipient; (2) sender's 'perceived agreement' was derived by comparing sender's anticipation of recipient's attitude vs. sender's reported attitude; and (3) 'sender's understanding of the recipient' was derived by comparing sender's anticipation of the recipient's attitude vs. recipient's reported attitude. Congruence scores were first calculated on the item-level. Scores for "enjoyable" and "appealing" were averaged to compose a "hedonic value" score; scores for "informative", "relevant", "interesting" were averaged to compose "utilitarian value" score. These composite scores were used for further analysis.

		Response A						
		strongly disagree			strongly agree			
		1	2	3	4	5	6	7
Response B	strongly disagree	1	10	9	7	5	3	2
		2	9	10	9	6	4	3
		3	7	9	10	8	5	4
		4	5	6	8	10	8	6
	strongly agree	5	3	4	5	8	10	9
		6	2	3	4	6	8	10
		7	1	2	3	5	7	9

Figure 16. Perceptual congruence scoring table (Benlian and Haffke 2015).

The construct recipient's satisfaction with online relationship was measured using 7-point semantic differential satisfaction scale of Bhattacharjee (2001) and included the following items: "How would you describe your experience with your friend on SNS?" – "very dissatisfied/very satisfied"; "very displeased/very pleased"; "very frustrated/very contented"; "absolutely terrible/absolutely delighted". Reflecting actual behaviour, positive feedback was assessed by asking recipients "Have you 'liked' the post of your friend? 'Liking' means clicking on the 'Like'-button or any other positive emoji e.g., laughing smiley" (1=yes, 0=no/I plan to do it). "Intention to ignore the content" was adopted from Peña and Brody (2014) and measured by asking "How likely

would you hide the posts of this SNS-friend? and “How likely would you ignore the posts of this SNS-friend? (1=very unlikely; 7=very likely). All constructs satisfied the criterion of internal consistency ($CA_{\text{satisfaction}}=0.869$, $CA_{\text{intent_to_ignore}}=0.757 > 0.7$).

Apart from gender, age and employment status, we also measured time spent on SNS as well as posting frequency to be able to describe our sample and to control for the effect of these variables. Time spent on SNS was measured by asking “How many minutes do you use Facebook/Instagram per day? (on average)”. The answers ranged from “less than 10 minutes” to “more than 3 hours” on a 6-point scale. Posting frequency was measured by asking “How often do you share a status update on Facebook/Instagram?” with eight response options ranging from “never” to “every day”. As the relationship of the dyadic partners differs, we also measured perceived closeness and communication frequency indicated by the recipient. Closeness was measured with one item “I have a very close relationship with this SNS connection” lent from Marsden and Campbell (1984). Communication frequency was measured with two items “I communicate regularly with this SNS connection (1) offline and (2) online”. Because attitudes and perceptions about network friends are sensitive in nature, we additionally controlled for the tendency to give socially desirable answers in our recipient sample by using the 13-item Marlowe-Crowne social desirability scale (Reynolds 1982). Spearman’s correlations between recipient’s satisfaction with online relationship, reported attitude of the recipient (regarding hedonic and utilitarian value of the content) and social desirability score of the recipients were insignificant. The same holds for Spearman’s correlations between sender’s reported attitude, sender’s anticipation of recipient’s perception (regarding hedonic and utilitarian value of the content) and social desirability score of the senders. We thus assume that our sample is not subject to a social desirability issue. Common method bias (Podsakoff et al. 2003) was measured by including the construct ‘tendency towards fantasizing’ (Son and Kim 2008) as a marker variable with the scale lent from Darrat et al. (2016): “I daydream a lot”, “When I go to the movies I find it easy to lose myself in the film” and “I often think of what might have been” (7-point Likert scale). To check for common method bias, we followed the guidelines by Rönkkö and Ylitalo (2011) and included the tendency to fantasize as a predictor for all endogenous constructs in our model (Figure 15). No significant regression paths became insignificant, suggesting that common method bias is not salient in our data.

Mann-Whitney U test applied to the dataset has shown that SNS type has no significant effect on the constructs (except one item *sender’s anticipation of the recipient’s attitude*_{appealing}, $U = -1.985$; $p = .047$), hence we decided not to split the sample by the platform. 65.56% of the respondents were female; the age ranged from 17 to 53 with the mean of 25.92 years. The majority of participants were either employed (52.78%) or students (34.44%).

Results

Hypotheses H1 and H2 were examined by the Mann-Whitney U test, which is a non-parametric equivalent of the independent samples t-test. It allows to compare differences between two groups accounting for the ordinal type and non-normal distribution of variables, which is the case for our perceptual constructs measured on a 7-point scale Likert scale or 10-point congruence scale. Our analysis reveals significant differences on reported value of the shared content between senders and recipients for both hedonic and utilitarian dimensions (H1a and H1b confirmed). In particular, senders perceive their own posts to be more *enjoyable* ($U = -2.534$; $p = .011$), *appealing* ($U = -3.663$; $p = .000$), *informative* ($U = -2.013$; $p = .044$), *relevant* ($U = -2.634$; $p = .008$) and *interesting* ($U = -2.115$; $p = .034$), as illustrated in Figure 17.

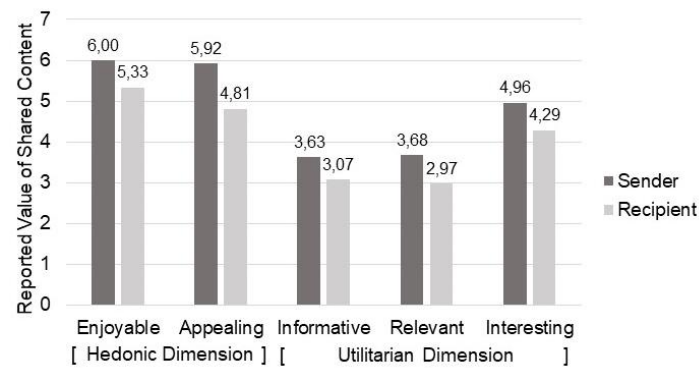


Figure 17. Mean values reported by senders and recipients (H1).

Comparison between actual agreement and sender's perceived agreement points out significant differences for utilitarian value ($U = -3.641$, $p = .000$) and for hedonic value ($U = -5.411$, $p = .000$). Similar to marital relationships (Acitelli et al. 1993), "false consensus effect" is present (Figure 18): senders who share content on an SNS anticipate that perceptions of recipients regarding shared content would be more similar to their own (with mean congruence score 8.54 for hedonic dimension and 8.24 for utilitarian dimension), than they actually are (with the mean congruence score 7.27 for hedonic dimension and 6.71 for utilitarian dimension) (H2a and H2b supported).

Differences between sender's perceived agreement (SPA) and actual agreement (AA) also hold on the item-level: senders anticipate that perceptions of recipients will be more similar to their own when rating their post in terms of it being *enjoyable* (mean SPA=8.69; mean AA=7.56; $U = -3.066$, $p = .002$), *appealing* (mean SPA=8.40; mean AA=6.99; $U = -3.488$; $p = .000$), *informative* (mean SPA=8.18; mean AA=6.66; $U = -3.577$; $p = .000$), *relevant* (mean SPA=8.31; mean AA=6.70; $U = -4.258$; $p = .000$), and *interesting* (mean SPA=8.22; mean AA=6.78; $U = -4.111$; $p = .000$), compared to the real degree of interpersonal perceptual congruence of the reported perceptions of senders and recipients (actual agreement).

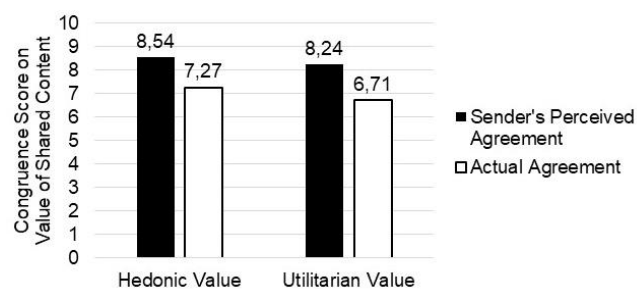


Figure 18. Congruence scores on actual agreement vs. perceived agreement (H2).

In our research model on the effects of sender's perceptual understanding of the recipient (Figure 19), we hypothesized that sender's understanding of the recipient regarding the value of the shared content contributes the recipient's satisfaction with online relationship, which in turn triggers a set of behavioral responses of the recipient. Our research model was evaluated using the partial least squares (PLS) with the help of the SmartPLS v.3.2.7 (C. M. Ringle et al. 2015). First, we assessed our measurement model by evaluating convergent and discriminant validity. To ensure convergent validity, parameters for indicator reliability (IR), composite reliability (CR) and Average Variance Extracted (AVE) were computed for two multi-item constructs in our model (recipient's satisfaction with online relationship; intention to ignore the content from this user). All item loading exceeded the 0.7 threshold (Hair et al. 2012), which provides assurance for the

IR. Further, CR values for both constructs were higher than the required level of 0.7 (Hair et al. 2012): $CR_{\text{satisfactionR}}=0.914$; $CR_{\text{intent_to_ignoreR}}=0.891$. The AVE values surpassed the threshold level of 0.5 (Quan-Haase and Young 2010): $AVE_{\text{satisfactionR}}=0.730$; $AVE_{\text{intent_to_ignoreR}}=0.804$. Hence, convergent validity can be assumed. The criterion for discriminant validity that compares the square root of AVE with inter-construct correlations was also fulfilled for our model (Hulland 1999, p. 200). Taken together, our measurement model is well-specified.

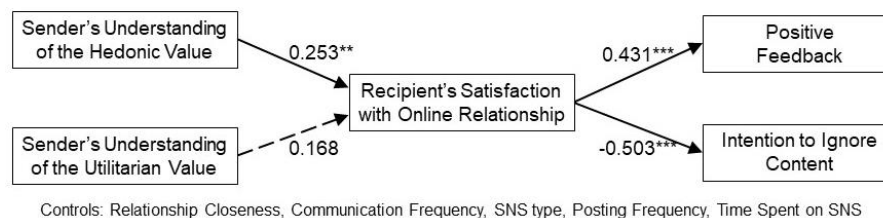


Figure 19. Results of the structural model testing (** $p < 0.001$, * $p < 0.01$).

In the next step, the Structural Model (SM) was evaluated by assessing the size of path coefficients and their significance via a bootstrapping procedure (see Figure 19). We find that the degree of sender's understanding regarding the hedonic value is positively associated with recipient's satisfaction with online relationship ($\beta=0.253$, $p=0.009$) thus supporting H3a. Understanding regarding the utilitarian value did not pass the significance threshold of 5% ($\beta=0.163$, $p=0.285$) and therefore H3b was rejected. Further, recipient's satisfaction with the online relationship is positively linked to the provision of positive feedback by clicking on the 'Like'-button ($\beta=0.431$, $p=0.000$), as well as to the intention to ignore the content of the sender ($\beta=-0.503$, $p=0.000$). Hence, H4a and H4b were supported in our sample. Finally, we controlled for the dyadic relationship and SNS usage. In line with past research (Cialdini et al. 1997; Savitsky et al. 2011), closeness positively affects recipient's satisfaction with the online relationship ($\beta=0.303^{**}$) and positive feedback ($\beta=0.255^{*}$) significantly. However, no path coefficient in the original model became insignificant by including this effect. Communication frequency, sender's/recipient's time spent on SNS, sender's posting activity and the type of SNS turned out to be insignificantly related to our three outcome variables. We discuss implications of our findings in the following section.

Discussion

In this section, we discuss our results by bridging them with related work and indicating our contribution for research and practice.—This study investigated the observed contradiction between perception of content contributors (senders) and content consumers (recipients) (Wenninger et al. 2016). While senders are typically well-meaning in their sharing, their content is often seen as irritating, annoying, envy-inducing, and excessive (e.g., Krasnova et al. 2015). In order to shed light on this obvious gap in intentions and perceptions, a dyadic study with 90 matched pairs of SNS users was conducted.

Implications for Research

This study adds to SNS research in several ways. First, our results provide a novel view on the undesirable consequences of content consumption for recipients on SNSs (Sasaki et al. 2016; Maier et al. 2015; Krasnova et al. 2015; Tandoc et al. 2015). Based on social cognition theory (Bandura 2002) and the perceptual congruence model (White 1985), we move beyond the one-sided investigation of sender's or recipient's perceptions in isolation; instead we focus on the interpersonal nature of SNS communication as we compare user perceptions in a dyadic setting.

This allows us to show that senders generally value their content more than recipients, scoring the hedonic and utilitarian value of the content higher. This conforms with recent findings indicating that recipients complain about needless and irrelevant information forced to them in their News Feed (Fox and Moreland 2015). Moving beyond the existence of perceptual differences, our results suggest that these contradictions occur due to senders' tendency towards egocentrism. Senders falsely anchored others' perception on their own building on the assumption that others are similar to them. We provide evidence that senders are biased, because perceived agreement (intrapersonal congruence of the sender) is significantly higher than actual agreement (interpersonal congruence of senders' and recipients' actual assessment). Along these lines, we support results of Kruger et al. (2005) that "false consensus" bias is even higher in electronic communication, which accentuates importance of perspective-taking. Senders are trapped by egocentrism while focusing on their own interests and needs (Barasch and Berger 2014). In this vein, we indicate that SNS artifacts like the invisible and heterogeneous audience coupled with asynchronous feedback leverages egocentrism and false-consensus bias compared to Face-to-Face communication. It challenges the ability of senders to put oneself in the shoes of others.

The need for perspective-taking brings us to our next contribution. Specifically, we show that sender's understanding of the recipient (accuracy of perspective-taking) influences relational outcomes. Subsequently, our findings highlight the critical importance of sender's understanding of the hedonic value of the content for the recipient. At the same time, contrary to our expectations, sender's understanding of the utilitarian value of the content for the recipient is not significantly related to relationship satisfaction. This result is plausible considering the hedonic orientation of SNSs, like Facebook or Instagram. We deem this finding as an indicator, that SNS environment are rather perceived as an environment for enjoyable pass time, which helps users to avoid boredom and supports them in their desire to procrastinate (Krasnova and Kift 2012; Kwak et al. 2014). This pleasure-oriented nature of SNSs stands in contrast with news websites aiming to inform people, or more goal-oriented professional networks like LinkedIn.

Finally, in line with marital relationship research (Levinger and Breedlove 1966; Schröder-Abé and Schütz 2011), our results yield insights that understanding between communication partners positively influences relationship satisfaction. In this regard, we are able to show that when senders perform better in terms of "stepping into the shoes" of their audiences, this will pay itself off socially as the sender is likely to enjoy more positive feedback, e.g., in the form of 'likes', and better acceptance of the shared content among its recipients. Together, our findings uncover, help explain and explore the consequences of perceptual incongruence between senders and recipients of content on SNSs.

Implications for Practice

There is a number of practical implications for SNS providers and users resulting from our study. First, senders should be aware that their anticipation of recipients' attitudes is biased in the direction of own perceptions, and is not fully reflective of the actual attitudes of the audience. Among others, social cognitive research explains that this may be due to differing emotional states (Van Boven and Loewenstein 2003). For instance, if someone shares content in a happy mood, it is hard to predict how people in a bad mood would react. Further, inaccuracies in perspective-taking can be reinforced by false positive feedback. While negative emoticons have been introduced on Facebook, most feedback still remains positive and may create the false impression that recipients actually like the content, whereas in reality 'likes' are often given on the basis of tie strength, or simply as a confirmation of seeing the content (Lee et al. 2016). Hence, platform

providers should be aware of this vicious cycle of positive feedback, and work towards mechanisms that counteract this dynamics.

Second, our results show that users who seek to be liked by their audience need to carefully think about the hedonic value of their content, since perceptions of hedonic value emerge as a critical driver of online relationship satisfaction, which in turn is positively associated with behavioral strategies favorable for a sender. This is in line with the results of Utz (2015) who shows that positive and entertaining content keeps the audience happy while contributing to the sense of connection.

For SNS providers who rely on user-generated content, fostering perspective-taking, for example by increasing awareness of its importance, emerges as an important strategy to ensure platform sustainability in the long-run. Indeed, if senders of content are not able to take the perspective of their audience, their recipients will in the worst case start ignoring their updates by hiding the content, which can backfire in terms of reduced time spent on an SNS in general. In this regard, no communication takes place as the shared content will not be visible to any recipient. Based on our results, we recommend SNS providers to strengthen other-focus on their platforms to enrich social interactions while keeping the communication loop of senders sharing content and recipients reacting on it stable. Already now, daily time spent on Facebook is less than 10 minutes – a significant decrease compared to just a few years ago (Alexa 2017).

Limitations and Future Research Suggestions

As with every research project, our study is subject to limitations. We asked dyads to respond to the questionnaire having the other person in mind. This allowed us to have real dyads with differing tie strength in our sample. In addition, we were able to capture interpersonal understanding on a post level. Although we assured the respondents that their data is treated anonymously and will not be shared with their friends, it is possible that respondents were biased as they had to provide private thoughts and opinions with regard to their friends or distant acquaintances. With respect to our results, we were not able to identify any social desirability bias, but it would be interesting to see whether future studies can replicate our results. An extension of our study with strangers indicating their perception of the content could lead to further interesting findings, as such research design will be less influenced by relationship closeness.

The survey was answered based on the latest post of the sender and related to one specific SNS connection. Certainly, users share different content over time and thus their accuracy in anticipating the perception of the value of the content for their peers might vary as well. In order to guide future research, we call for studies to investigate the factors that influence understanding. Our study revealed that understanding is crucial on SNS, but its antecedents remain unclear. Additionally, it could be also fruitful to analyze the divergence between actual and perceived agreement, and to further explore the determinants and consequences of false consensus bias on SNSs.

Finally, we conducted a survey among Instagram and Facebook users. However, one could expect that interpersonal perceptions and their impact on other platforms might differ. For instance, it is possible that on professional SNSs like LinkedIn utilitarian understanding positively impacts recipient's satisfaction with the online relationship.

Conclusion

Inaccuracy in perspective-taking is a common concern of interpersonal communication. Similar to traditional writing where audience is often unknown to the sender, “broadcasting” to wide audience on SNSs requires ability to understand the potential readers in order to succeed. Our results provide insights on the bilateral perceptions of content that is shared on SNS. Senders’ accurate anticipation of recipients’ perceptions of the shared content can leverage a healthy SNS environment. In contrast, misunderstanding can lead to reluctance to follow the content on the part of the receiving audiences, thereby threatening to undermine the sustainability of SNSs. Together, our findings contribute to a better understanding of the underlying dynamics of content sharing and consumption on SNSs, and have significant implications for theory and practice.

11 Overarching Findings and Discussion

To take advantage of information systems such as social networking sites, online shopping or other online services, users often have to disclose a number of personal information. This leads them to express high privacy risks, as they feel that they lose control over the use and dissemination of their data (Auxier et al. 2019). The IS privacy literature predominantly assumes that Internet users will use an information system if its benefits outweigh the privacy risks (Abramova et al. 2017; Krasnova et al. 2010a; Li 2012). This rational trade-off is referred to as the privacy calculus (Culnan and Armstrong 1999; Dinev and Hart 2006; Laufer and Wolfe 1977). However, observation of actual behavior shows that Internet users sometimes also reject a service even though it is privacy-friendly (Gerlach et al. 2019) or use a service despite its intrusiveness (Alashoor and Baskerville 2015; Brakemeier et al. 2016a). This is in contradiction to the privacy calculus. In fact, actual disclosure decisions seem to be influenced by situational factors such as affect, immediate gratification, bounded rationality, as well as the general context in which they are made (i.e., SNS, data-selling platforms etc.) (Dinev et al. 2015). Thus, current research only offers an incomplete picture of Internet users' self-disclosure decisions.

This thesis main goal is to establish a deeper understanding of the formation of Internet users' self-disclosure decisions in light of the privacy calculus. In particular, the sole focus on privacy risks and benefits underlying the privacy calculus is extended. Even though the existence of the privacy calculus is supported by many empirical studies (e.g., Krasnova et al. 2010a, Xu et al. 2009), it often fails in explaining actual self-disclosure decisions and ultimately provide scattered results. Motivated by the lack of empirical explanations for scattered or even contradictory research results, it is of great importance to understand the dynamics behind self-disclosure for users, firms and policymakers. Understanding situational factors which affect self-disclosure is crucial when designing innovative technologies that rely on user data, or providing initiatives that protect users' data. To reach this goal, six quantitative studies along with two structured literature reviews and two qualitative pre-studies are conducted. Across varying contexts like data marketplaces, social networking sites, and other smartphone applications, Internet users' privacy-related judgements of online companies are examined. All studies are stemming from the assumption that the privacy risk-benefit analysis underlying the privacy calculus is oversimplified and thus does not reflect real disclosure behavior. In an attempt to identify additional nuances of self-disclosure decision-making, (1a) the antecedents of user's willingness-to-sell personal information as well as (1b) distributive equity perceptions of data-driven online companies have been assessed, (2) overconfidence and evaluability mode have been identified to moderate the link between privacy risks and self-disclosure, and (3) social concerns have been found to impede self-disclosure decision-making beyond privacy concerns. The extension of the privacy calculus are shown in the following Figure:

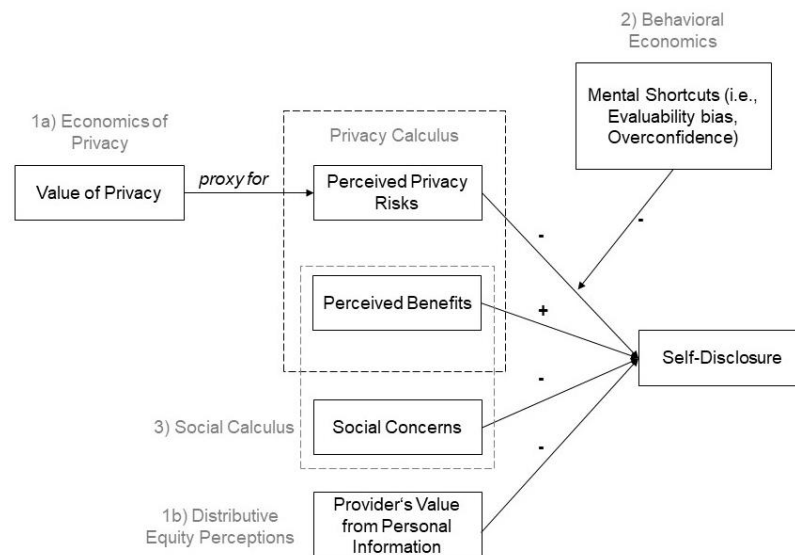


Figure 20. Extension of the privacy calculus model with additional factors.

By integrating theories stemming from other research fields into the privacy calculus (see Figure 20 above), the privacy risk-benefit analysis has been extended by factors such as social concerns that replace privacy risks on SNS and mental shortcuts (like overconfidence) that distort the causal link between privacy risks and self-disclosure and thus lead to an irrational disclosure decision. To sum up, this thesis shows that the privacy calculus needs to be extended by other factors than benefits and privacy risks as depicted in Figure 20 in order to provide a deeper understanding of the factors that determine self-disclosure behavior in different contexts; sometimes even evidencing that privacy risk play no role at all. Extending the privacy calculus and thus reflecting individuals' complex self-disclosure decision-making has got implications for research, individuals, organizations and policymakers, because it enhances privacy literature, protection and its legislation.

Theoretical Contributions

Overall, responding to the three overarching research questions, this thesis incorporated three different perspectives into the privacy calculus: (1) value-based approach, (2) cognitive and behavioral biases, and (3) social parameters. These perspectives determine the order of this thesis' contributions expressed in the following.

The first three research papers (1.A, 1.B., 1.C) are devoted to the research theme 'value of privacy' as a proxy for Internet users' perceived privacy risks. These papers aim at clarifying what drives valuation of personal information and how it relates to the monetization extent of data-driven service providers from a user perspective. Starting off with a literature review, the first article presents a theoretical framework highlighting antecedents, research methods, and the value Internet users place on their privacy based on the results of 37 studies in different contexts. The corresponding literature framework shows that Internet users value their personal information differently depending on the context like type of information requested, data collector, and other situational factors. Beyond that, research merely focused on the investigation of individuals' willingness to protect instead of peoples' willingness to sell their data.

Based on the results of this structured literature review, the second paper's goal was to identify antecedents of individuals' willingness to sell their personal information and their relative importance based on a context-independent study design. Since current research results are

scattered and differ across contexts, a more neutral setting – namely data selling platforms - was necessary in order to provide more generalizable results. Together with the benefits of a qualitative pre-study, a conjoint-analysis shows that the amount of compensation, type of data collector, and its origin are the key factors influencing individuals' willingness to sell their privacy.

The third article deals with users' perception of provider's net value from personal information. Specifically, it revolves around the question in how far Internet users incorporate the value for the provider in their distributive equity assessment, which in turn affects satisfaction and continuance intention. Based on equity theory, the relationship between data-driven service providers and users is characterized as a bidirectional exchange process where values are transmitted from users to providers and vice versa. Thus, this study complements research on users' perception of value of privacy by extending the privacy calculus model by users' perception of providers' value from personal information. It shows that users do not only account for a fair data handling process but also for a fair value distribution between them and providers in order to establish a long-term relationship.

Research paper 2.A and 2.B are devoted to the investigation of reasons for irrational, unstable or sometimes paradoxical privacy-related judgements with regard to actual self-disclosure behavior. Since behavioral economics literature explains peoples' mental shortcuts and thus deviations from rational decision-making, two biases stemming from this literature stream have been tested as potential moderators of the privacy risk-self-disclosure link. Both biases help explain why self-disclosure decision making is not stable and uniquely across contexts. In fact, it is dependent on the framing of alternatives and Internet users' overconfidence of their privacy knowledge. Thus, the privacy calculus is simplifying the cognitive and behavioral mechanisms behind self-disclosure. In this regard, both research papers contribute to studies investigating paradoxical privacy decisions (Adjerid et al. 2018; Alashoor and Baskerville 2015; Brakemeier et al. 2016a; Gerlach et al. 2019) and ultimately provide a more nuanced picture of self-disclosure decisions. Based on these results, studies adopting a privacy calculus lens should consider that their respondents might be biased due to overestimation of their privacy knowledge or missing reference information.

Finally, the last three research papers (3.A, 3.B, 3.C) are centered on social components of sharing personal information on SNS. First, a structured literature review was conducted which identified self-presentation and enjoyment as the major driver while perceived privacy risks or sometimes concerns constitute the most prominent impediment to self-disclosure on SNS. Thus, the literature review shows that the privacy calculus is the predominantly applied theory to describe disclosure behavior. However, interpersonal communication theory argues that when communicating to other individuals users perceive social concerns like fear of being negatively evaluated. Indeed, in article 3.B a qualitative pre-study evidences that social concerns are even more decisive for SNS users than privacy-related fears. Based on these results, the privacy calculus is extended by a social perspective in article 3.B whereas not only privacy concerns account for individuals' worry when self-disclosing but also social concerns like being perceived as a braggart. These concerns are especially salient in online communication where the perception of others' reactions and emotions is disturbed due to delayed feedback and its one-sided nature ('Like'-button only).

Research paper 3.C digs deeper into individuals' social concerns by investigating in how far senders on SNS overestimate/underestimate positive/negative perceptions evoked in their audience based on a dyadic study. Among others, the results highlight that users who share status updates overestimate the extent to which their messages are perceived as entertaining by their

recipients because they are unable to empathize with them and in turn not accurately predict their perceptions. In this regard, they are subject to a perspective-taking bias. To conclude, these three research papers argue that the privacy calculus needs to be contextualized for the SNS environment where privacy risks play a less significant role than social concerns.

Taken together, all this thesis' findings confirm that self-disclosure decisions are complex in nature and are highly depending on the context (e.g., availability of alternatives) in which they are made. In this vein, the results of this cumulative dissertation pursue one of the most critical factors of the information age, namely users' privacy protection. Making it short, self-disclosure decisions are not always a result of a deliberate and cautious information processing solely based on an assessment of privacy risks and benefits as merely assumed in IS research. Based on this thesis' results, the well-established privacy calculus needs to be extended by the following perceptions as well as cognitive and behavioral biases:

- Perceived monetary amount of compensation, type of data requested, and origin of the data-driven business provider as major antecedents for users' value of privacy
- Distributive equity perceptions, expressed by the value from personal information for the provider
- Evaluability bias determined by the availability of reference information
- Overconfidence caused by an overestimation of ones' privacy knowledge
- Social concerns conceptualized as the fear of being negatively evaluated by others

Limitations and future research suggestions stemming from these results are provided in the respective publication.

Practical Contributions

Making self-disclosure decisions is a difficult and complex task for Internet users in the digital age. Among others, it is determined by their value of privacy, benefits offered in return, perceptions of providers' value from personal information, social concerns, as well as privacy risks along with its mental shortcuts. Explaining the dynamics and mechanisms behind Internet users' self-disclosure decisions is not only of high importance for researchers, but also for firms, policymakers and individuals. For firms, users' self-disclosure is crucial in order to personalize products or invent new ones. For example, online retailers can show their customers targeted products that they might like based on their analysis of customers' purchase history. Thus, the magnitude of users' privacy concerns is a key indicator in order to subsume the degree to which personal information can be used for personalization and marketing purposes without putting customers' loyalty and acquisition at risk. In other words, firms need to keep track of their evoked privacy concerns and users' perception of the monetization extent of their personal information in order to offer equivalent service benefits in return. Otherwise, users will feel that values are unfairly distributed between them and firms and in turn are dissatisfied with the service, eventually causing a service rejection. At the same time, firms should compare their privacy practices with other competitors, because in joint evaluation mode, customers' perceive higher privacy risks attributed to the provider which gathers more data. Reversely, this means if individuals understand organizations' privacy practices, it is incorporated into their decision-making. In other words, the more users know about the processing of their data, the more they use a service and disclose their data to that service provider (Staddon et al. 2012). Thus, by being transparent about their data practices organizations can gain competitive advantage and thus long-term customer loyalty. However,

there will always be a conflict about minimizing privacy violations while maximizing data collection by firms.

Against this background, privacy-friendly service providers should educate their potential users to help them to understand and in turn consider privacy features to make privacy intelligent disclosure as well as usage decisions. In other words, Internet users need to be aware of the privacy-friendliness of these systems, because otherwise it is not taken into account when making a disclosure decision. More specifically, this thesis identified two biases which should be addressed by privacy-friendly providers. First, in order to overcome individuals' overconfidence bias, Internet users need to be trained to leverage their knowledge and capabilities to make informed privacy decisions that are stable over time. Second, to mitigate the effect of an evaluability bias, privacy-friendly service providers should always present reference information next to their offer. For instance, they can highlight that they collect less personal information compared to competitors or display privacy seals. In this regard, Internet users are more likely to undergo a privacy risk analysis and thus privacy friendliness becomes indeed a competitive advantage.

For SNS providers this thesis' results offer explanations why users sometimes refrain from sharing personal information even though they perceive high benefits and low privacy risks. In addition to privacy concerns, information sharing on SNS seems to be inhibited by social concerns (i.e., fear of being negatively evaluated by others). In this regard, this thesis provides recommendations to help SNS providers to diminish users' social concerns by building awareness about privacy functionalities and self-presentation dilemmas. For instance, with a large-scale image campaign, Facebook started to clarify the aspects of privacy in their social network. Facebook advertised with photos of users who have publicly shared personal information - supposedly from cluelessness - which they later regretted with regard to social threats or privacy concerns. According to the title of the campaign "Make Facebook your Facebook", Facebook aimed at engaging their users to use the privacy settings and features in terms of deleting previous posts, limiting the audience, and to enlighten the complexity of the communication platform (Facebook 2021). All in all, SNS providers should further increase users' knowledge about such functionalities in order to avoid regret of self-disclosure or other social punishments (e.g., cyberbullying, offline gossip, unfriending etc.) which might lead to less content being shared on these platforms in the long-run.

For governments, the magnitude of disclosure of personal information should be of utmost interest as it is a major driver of economic growth. Indeed, "IT analysts predicted that technology companies may severely suffer economically if citizens and businesses withdrew their use of cloud data storage, social networks such as Facebook, Twitter, Instagram, or user data-intensive companies such as Google, Microsoft, and Apple." (Dinev 2014, p. 97). If individuals are unwilling to share their personal information, it might hinder digital innovativeness which relies on personal information being shared. In order to protect Internet users' privacy online, the EU issued the GDPR, but since privacy violations are still an ongoing issue and privacy breaches are on the rise, policymakers should continuously track whether their regulations meet the constantly changing privacy practices of online companies. In fact, an international poll has shown that only 50 percent of Internet users across more than 25 countries believe that their governments do enough to protect Internet users' privacy (CIGI 2019). Thus, this thesis' results are valuable for governments and policymakers for finding the right balance between minimizing privacy valuations for users and maximizing digital innovativeness based on personal data. For instance,

they can learn from this thesis' results in which cases privacy plays a role in users' decision making and ultimately needs to be protected by legislative rules.

For Internet users, this thesis identified three cognitive biases users need to be aware of when deciding to self-disclose. First, evaluability bias has been shown to diminish in how far privacy risks are incorporated in individuals' decision-making. In single evaluation mode, users' are unable to assess the privacy risks evoked by an information system because no reference information is provided. When no reference information such as the personal information requested by a competitor is available, users are not confident in their privacy risk assessment and thus they have a lower disposition to their perceived risks. Second, Internet users are subject to an overconfidence bias, because when overestimating their privacy knowledge this leads to a less rational privacy decision-making. Resulting from these biases, Internet users do not make stable privacy decisions against the background of their preferences. Being aware of users' pitfalls, malicious organizations can exploit users' data in ways they have not foreseen it. Third, SNS users are fraught by a perspective-taking bias which makes it hard for them to predict the actual feelings and perceptions caused by their own shared content on the recipient side. Heterogeneous audience, asynchronous and limited feedback challenges intelligent self-disclosure since users overestimate the extent of positive perceptions while underestimating negative perceptions evoked by their messages.

In the end, Internet users need to be aware of their cognitive shortcomings as it is up to each user to decide whether to disclose their personal information against the background of their own privacy preferences. Idealistically, users should be able to negotiate the disclosure of their personal information. However, Internet users will always feel the tension of being able to use new technologies which require personal information in order to provide their full functionalities and their wish to protect their information privacy. Even though this tension cannot be nullified users should be able to take their perceived privacy risks into consideration and make intelligent self-disclosure decisions which are perceived as fair, are not regretted or exploited by malicious organizations.

12 Concluding Remarks

Online self-disclosure is ubiquitous in today's digitized world. Although it provides benefits like monetary rewards, personalization or social advantages, it comes at the price of losing control over one's privacy. This cumulative thesis along with its 6 large-scale quantitative studies, two literature reviews, and qualitative pre-studies sheds light into the complex dynamics of online self-disclosure. It makes an important contribution to Information Systems research by broadening the understanding of scattered results based on the privacy calculus. Specifically, by combining behavioral economics, interpersonal communication theory and established value measurement methods with privacy research, the rational self-disclosure trade-off between benefits and privacy risks is extended. All in all, a more nuanced model of self-disclosure online is developed.

I hope that future research can build on these results and take them into account when studying self-disclosure decisions. Apart from the future research suggestions that have already been stated in each research paper forming this thesis, the following ideas may be valuable for upcoming research projects. First, among others this thesis builds on behavioral economics to explore cognitive as well as behavioral biases which lead to irrational disclosure decisions. However, literature investigating bounded privacy-related decision making is still in its infancy (e.g., Adjerid et al. 2018; Gerlach et al. 2019) and thus more research is necessary to understand situational factors which jeopardize the rational risk-benefit analysis (Dinev et al. 2015). In this vein, longitudinal studies could offer further insights on users' complex and context-dependent self-disclosure decisions (Wagner et al. 2021).

Second, with the advent of sophisticated technologies such as artificial intelligence (AI) new privacy issues come to the spotlight (Li and Zhang 2017). For example, facial recognition can identify and ultimately surveil users in public spaces without their consent and thus gather information of people who aim to stay anonymous. Beyond that, AI applications can be used to re-identify users in big data sets to infer and generate sensitive information from anonymized data sets (El Emam et al. 2011). This implies that individuals are faced with the challenge to fully understand when data is gathered, and how it can be used for unwanted purposes like profiling, surveillance, or data exploitation. Therefore, more research is necessary to investigate how privacy risks, norms, and beliefs evolve over time. At the same time, it would be fruitful to dig deeper into the effectiveness of privacy education which might help Internet users to make intelligent disclosure choices. In this regard, research can build on techniques like debiasing, feedback, warning or generally nudging (Acquisti et al. 2017) to identify mechanisms which leverage intelligent disclosure decisions. Moreover, the studies included in this thesis focused on users' perceptions of providers' misuse of personal information. Studying privacy risks stemming from other users could be another interesting research angle which is underdeveloped in privacy research to date (Bélanger and James 2020). To conclude, since privacy decisions, protection, and legislation are at center stage, more research is valuable to understand the full complexity of disclosure decisions against the background of sophisticated technologies and mental shortcuts.

References

- Abramova, O., Wagner, A., Krasnova, H., and Buxmann, P. 2017. "Understanding Self-Disclosure on Social Networking Sites - A Literature Review," in *Proceedings of the 23rd Americas Conference of Information Systems*.
- Accenture. 2015. "Guarding and Growing Personal Data Value." (https://www.accenture.com/_acnmedia/PDF-4/Accenture-Guarding-and-Growing-Personal-Data-Value-POV-Low-Res.pdf).
- Acitelli, L. K., Douvan, E., and Veroff, J. 1993. "Perceptions of Conflict in the First Year of Marriage: How Important Are Similarity and Understanding?," *Journal of Social and Personal Relationships*, pp. 5–19.
- Acquisiti, A., and Gross, R. 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," *International Workshop on Privacy Enhancing Technologies, Springer, Berlin*, pp. 36–58.
- Acquisti, A. 2004. "Privacy in Electronic Commerce and the Economics of Immediate Gratification," in *Proceedings of the 5th ACM Conference on Electronic Commerce - EC '04*.
- Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., and Wilson, S. 2017. "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online," *ACM Computing Surveys* (50:3).
- Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. "Age of Information," *Science* (347:6221), pp. 509–515.
- Acquisti, A., and Grossklags, J. 2005a. "Privacy and Rationality in Individual Decision Making," *IEEE Security and Privacy* (3:1), pp. 26–33.
- Acquisti, A., and Grossklags, J. 2005b. "Uncertainty, Ambiguity and Privacy," in *Proceedings of the 4th Annual Workshop on Economics and Information Security*, pp. 1–21.
- Acquisti, A., John, L. K., and Loewenstein, G. 2013. "What Is Privacy Worth?," *Journal of Legal Studies* (42:2), pp. 249–274.
- Acquisti, A., John, L., and Loewenstein, G. 2009. "What Is Privacy Worth?," in *Proceedings of the Workshop on Information Systems and Economics*.
- Adams, J. S. 1965. "Inequity in Social Exchange," in *Advances in Experimental Social Psychology* (2nd ed.), L. Berkowitz (ed.), New York, NY: Academic Press, pp. 267–299.
- Adjerid, I., Peer, E., and Acquisti, A. 2018. "Beyond The Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making," *MIS Quarterly* (42:2), pp. 465–488.
- Aggarwal, R., Kryscynski, D., Midha, V., and Singh, H. 2015. "Early to Adopt and Early to Discontinue: The Impact of Self-Perceived and Actual IT-Knowledge on Technology Use Behaviors of End Users," *Information Systems Research* (26:1), pp. 127–144.

- Aharony, N. 2016. "Relationships among Attachment Theory, Social Capital Perspective, Personality Characteristics, and Facebook Self-Disclosure," *Journal of Information Management* (68:3), pp. 362–386.
- Ahmed, A. A.-A. M. 2015. "'Sharing Is Caring': Online Self-Disclosure, Offline Social Support, and Social Network Site Usage in the UAE," *Contemporary Review of the Middle East* (2:3), pp. 192–219.
- Aïmeur, E., Lawani, O., and Dalkir, K. 2016. "When Changing the Look of Privacy Policies Affects User Trust: An Experimental Study," *Computers in Human Behavior* (58), Elsevier Ltd, pp. 368–379.
- Alashoor, T., and Baskerville, R. 2015. "The Privacy Paradox: The Role of Cognitive Absorption in the Social Networking Activity," in *Proceedings of the 36th International Conference on Information Systems*.
- Alexa. 2017. "How Engaged Are Visitors to Facebook.Com?" (<https://www.alexa.com/siteinfo/facebook.com>).
- Allen, A., and Thompson, T. 1984. "Agreement, Understanding, Realization, and Feeling Understood as Predictors of Communicative Satisfaction in Marital Dyads," *Journal of Marriage and Family* (46:4), pp. 915–921.
- Alloway, T., Runac, R., Qureshi, M., and Kemp, G. 2014. "Is Facebook Linked to Selfishness? Investigating the Relationships among Social Media Use, Empathy, and Narcissism," *Social Networking* (3), pp. 150–158.
- Alter, S. 2009. "Mapping the Domain of Service Science," in *Proceedings of the 15th Americas Conference on Information Systems*.
- Ament, C. 2017. "The Ubiquitous Security Expert: Overconfidence in Information Security," in *Proceedings of the International Conference on Information Systems*.
- Ament, C., and Jaeger, L. 2017. "Unconscious on Their Own Ignorance: Overconfidence in Information Security," in *Proceedings of Pacific Asia Conference on Information Systems*.
- Anderson, M., and Jiang, J. 2018. "Teens' Social Media Habits and Experiences," *Pew Research Center*. (<https://www.pewresearch.org/internet/2018/11/28/teens-social-media-habits-and-experiences/>, accessed February 2, 2020).
- Anderson, M., and Vogels, E. A. 2020. "Americans Turn to Technology During COVID-19 Outbreak, Say an Outage Would Be A Problem," *Pew Research Center*. (<https://www.pewresearch.org/fact-tank/2020/03/31/americans-turn-to-technology-during-covid-19-outbreak-say-an-outage-would-be-a-problem/>, accessed January 22, 2021).
- Anderson, R. E., and Srinivasan, S. S. 2003. "E-Satisfaction and E-Loyalty: A Contingency Framework," *Psychology and Marketing* (20:2), pp. 123–138.
- Angst, C. M., and Agarwal, R. 2009. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MIS Quarterly* (33:2), pp. 339–370.
- Aperjis, C., and Huberman, B. A. 2012. "A Market for Unbiased Private Data: Paying Individuals According to Their Privacy Attitudes," *First Monday* (17:5).
- Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., and Turner, E. 2019. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," *Pew*

- Research Center. (<https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>).
- Aviram, H. 2012. "What Would You Do? Conducting Web-Based Factorial Vignette Surveys," in *Handbook of Survey Methodology for the Social Sciences*, G. (ed.) (ed.), New York, NY: Springer, pp. 463–473.
- Awad, N. F., and Krishnan, M. S. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization," *MIS Quarterly* (30:1), pp. 13–28.
- Baek, Y. M., Kim, E. M., and Bae, Y. 2014. "My Privacy Is Okay, But Theirs Is Endangered: Why Comparative Optimism Matters in Online Privacy Concerns," *Computers in Human Behavior* (31:1), Elsevier Ltd, pp. 48–56.
- Bagozzi, R. P., and Yi, Y. 1989. "On the Use of Structural Equation Models in Experimental Designs," *Journal of Marketing Research* (26:3), SAGE Publications, pp. 271–284.
- Bagozzi, R. P., and Yi, Y. 2012. "Specification, Evaluation, and Interpretation of Structural Equation Models," *Journal of the Academy of Marketing Science* (40:1), pp. 8–34.
- Bal, G. 2014. "Designing Privacy Indicators for Smartphone App Markets: A New Perspective on the Nature of Privacy Risks of Apps," in *Proceedings of the Americas Conference on Information Systems*.
- Bandura, A. 1986. *Foundations of Thought and Action: A Social Cognitive Theory*, Englewood Cliffs, NJ: Prentice-Hall.
- Bandura, A. 2002. "Media Effects: Advances in Theory and Research," in *Social Cognitive Theory of Mass Communication*, pp. 94–124.
- Bansal, G., Zahedi, F. M., and Gefen, D. 2010. "The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online," *Decision Support Systems* (49:2), North-Holland, pp. 138–150.
- Bansal, G., Zahedi, F. M., and Gefen, D. 2016. "Do Context and Personality Matter? Trust and Privacy Concerns in Disclosing Private Information Online," *Information and Management* (53:1), Elsevier, pp. 1–21.
- Barak, O., Cohen, G., Gazit, A., and Toch, E. 2013. "The Price Is Right? Economic Value of Location Sharing," in *Proceedings of the 2nd ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication*, Zurich, CH, pp. 891–899.
- Barasch, A., and Berger, J. 2014. "Broadcasting and Narrowcasting: How Audience Size Affects What People Share," *Journal of Marketing Research* (51:3), pp. 286–299.
- Barnes Jr., J. H. 1984. "Cognitive Biases and Their Impact on Strategic Planning," *Strategic Management Journal* (5), pp. 129–137.
- Baron, R. M., and Kenny, D. A. 1986. "The Moderator–Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations," *Journal of Personality and Social Psychology* (51:6), pp. 1173–1182.
- Bateman, P. J., Pike, J. C., and Butler, B. S. 2011. "To Disclose or Not: Publicness in Social Networking Sites," *Information Technology & People* (24:1), pp. 78–100.

- Bauer, C., Korunovska, J., and Spiekermann, S. 2012. "On the Value of Information - What Facebook Users Are Willing To Pay," in *Proceedings of 20th European Conference on Information Systems*.
- Baumeister, R. F., and Leary, M. R. 1995. "The Need to Belong: Desire for Interpersonal Attachments as a Fundamental Human Motivation," *Psychological Bulletin* (117:3), pp. 497–529.
- Baumeister, R., and Leary, M. 1997. "Writing Narrative Literature Reviews," *Review of General Psychology* (1:3), pp. 311–320.
- Bazarova, N. N., and Choi, Y. H. 2014. "Self-Disclosure in Social Media: Extending the Functional Approach to Disclosure Motivations and Characteristics on Social Network Sites," *Journal of Communication* (64:4), pp. 635–657.
- Bazerman, M. H., Moore, D. A., Tenbrunsel, A. E., Wade-Benzoni, K. A., and Blount, S. 1999. "Explaining How Preferences Change Across Joint Versus Separate Evaluation," *Journal of Economic Behavior and Organization* (39:1), Elsevier, pp. 41–58.
- Becker, G. M., DeGroot, M. H., and Marschak, J. 1964. "Measuring Utility By a Single-Response Sequential Method," *Systems Research & Behavioral Science* (9:3), pp. 226–232.
- Bélanger, F., and Carter, L. 2008. "Trust and Risk in E-Government Adoption," *Journal of Strategic Information Systems* (17:2), pp. 165–176.
- Bélanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy," *MIS Quarterly* (35:4), pp. 1–36.
- Bélanger, F., and James, T. L. 2020. "A Theory of Multilevel Information Privacy Management for the Digital Era," *Information Systems Research* (31:2), pp. 510–536.
- Benlian, A. 2014. "Are We Aligned...Enough? The Effects of Perceptual Congruence Between Service Teams and Their Leaders on Team Performance," *Journal of Service Research* (17:2), pp. 212–228.
- Benlian, A., and Haffke, I. 2015. "Does Mutuality Matter? Examining the Bilateral Nature and Effects of CEO-CIO Mutual Understanding," *Journal of Strategic Information Systems* (25:2), Elsevier B.V., pp. 104–126.
- Benndorf, V., and Normann, H.-T. 2014. "The Willingness to Sell Personal Data," *DICE Discussion Paper*.
- Beresford, A. R., Kübler, D., and Preibusch, S. 2012. "Unwillingness to Pay for Privacy: A Field Experiment," *Economics Letters* (117:1), pp. 25–27.
- Berlo, D. K. 1960. *The Process of Communication: An Introduction to Theory and Practice*, (Hott, ed.), New York: Rinehart, & Winston.
- Berman, J. Z., Levine, E. E., Barasch, A., and Small, D. A. 2015. "The Braggart's Dilemma: On the Social Rewards and Penalties of Advertising Prosocial Behavior," *Journal of Marketing Research* (52:1), pp. 90–104.
- Bernstein, M. S., Bakshy, E., Burke, M., Karrer, B., and Park, M. 2013. "Quantifying the Invisible Audience in Social Networks," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Vol. 3), pp. 21–30.
- Bevan-Dye, L., and Akpojivi, U. 2015. "South African Generation Y Students' Self-Disclosure on Facebook," *South African Journal of Psychology* (46:1), pp. 114–129.

- Bhattacharjee, A. 2001. "Understanding Information Systems Continuance: An Expectation-Confirmation Model," *MIS Quarterly* (25:3), pp. 351–370.
- Błachnio, A., Przepiorka, A., Bałakier, E., and Boruch, W. 2016. "Who Discloses the Most on Facebook," *Computers in Human Behavior* (55), pp. 664–667.
- Boldt, A., de Gardelle, V., and Yeung, N. 2017. "The Impact of Evidence Reliability on Sensitivity and Bias in Decision Confidence," *Journal of Experimental Psychology: Human Perception and Performance* (43:8), American Psychological Association Inc., pp. 1520–1531.
- De Bondt, W. F. M., and Thaler, R. H. 1995. "Financial Decision-Making in Markets and Firms: A Behavioral Perspective," *Handbooks in Operations Research and Management Science* (Vol. 9).
- Van Boven, L., and Loewenstein, G. 2003. "Social Projection of Transient Drive States," *Personality & Social Psychology Bulletin* (29:9), pp. 1159–68.
- Van Boven, L., and Loewenstein, G. 2005. "Empathy Gaps in Emotional Perspective Taking," in *Other Minds: How Humans Bridge the Divide Between Self and Others*, New York: Guilford Press, pp. 284–297.
- Boyd, D., and Ellison, N. B. 2008. "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication* (13), pp. 210–230.
- Boyd, D., and Heer, J. 2006. "Profiles as Conversation: Networked Identity Performance on Friendster," in *Proceedings of the Annual Hawaii International Conference on System Sciences*.
- Brakemeier, H., Wagner, A., and Buxmann, P. 2017. "When Risk Perceptions Are Nothing But Guesses – An Evaluability Perspective on Privacy Risks," in *Proceedings of the 38th International Conference on Information Systems*.
- Brakemeier, H., Widjaja, T., and Buxmann, P. 2016a. "Calculating with Different Goals in Mind - The Moderating Role of the Regulatory Focus in the Privacy Calculus," in *Proceedings of the European Conference in Information Systems*.
- Brakemeier, H., Widjaja, T., and Buxmann, P. 2016b. "Distinguishing Usage and Disclosure Intentions in Privacy Research: How Our Two Selves Bring About Differences in the Effects of Benefits and Risks," *Proceedings of the European Conference on Information Systems*.
- Brandimarte, L., and Acquisti, A. 2012. "The Economics of Privacy," *Handbook of the Digital Economy*, (ed. M. Peitz and J. Waldfoegel, ed.), New York: Oxford University Press.
- Braun, A., Schmeiser, H., and Schreiber, F. 2016. "On Consumer Preferences and the Willingness to Pay for Term Life Insurance," *European Journal of Operational Research* (25:3), pp. 761–776.
- Breidert, C., Hahsler, M., and Reutterer, T. 2006. "Willingness-To-Pay," *Innovative Marketing* (2:4), pp. 8–32.
- Bright, L. F., Kleiser, S. B., and Grau, S. L. 2015. "Too Much Facebook? An Exploratory Examination of Social Media Fatigue," *Computers in Human Behavior* (44), pp. 148–155.
- von Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., Cleven, A., Brocke, J. Von, and Reimer, K. 2009. "Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process," in *Proceedings of the 17th European Conference on Information Systems*.
- Brook, J. S., Whiteman, M., and Cohen, P. 1995. "Stage of Drug Use, Aggression, and Theft/Vandalism: Shared and Unshared Risks," in *Drugs, Crime, and Other Deviant Adaptions*:

- Longitudinal Studies*, H. B. Kaplan (ed.), New York: Springer Science and Business Media, pp. 83–96.
- Brush, A. J. B., Krumm, J., and Scott, J. 2010. "Exploring End User Preferences for Location Obfuscation, Location-Based Services, and the Value of Location," in *Proceedings of the 12th ACM International Conference on Ubiquitous Computing*, pp. 95–104.
- Buckman, J. R., Bockstedt, J. C., and Hashim, M. J. 2019. "Relative Privacy Valuations Under Varying Disclosure Characteristics," *Information Systems Research* (30:2), pp. 375–388.
- Bughin, J. 2011. "Digital User Segmentation and Privacy Concerns," *Journal of Direct, Data and Digital Marketing Practice* (13:2), pp. 156–165.
- Buller, D. B., and Burgoon, J. K. 1996. "Interpersonal Deception Theory," *Communication Theory* (6:3), pp. 203–242.
- Burke, M., Marlow, C., and Lento, T. 2010. "Social Network Activity and Social Well-Being," in *Proceedings of the Conference on Human Factors in Computing Systems*.
- Burson, K. A., Larrick, R. P., and Klayman, J. 2006. "Skilled or Unskilled, but Still Unaware of It: How Perceptions of Difficulty Drive Miscalibration in Relative Comparisons," *Journal of Personality and Social Psychology* (90:1), pp. 60–77.
- Busenitz, L. W. 1999. "Entrepreneurial Risk and Strategic Decision Making," *The Journal of Applied Behavioral Science* (35:3), pp. 325–340.
- Cardozo, R. N. 1965. "An Experimental Study of Customer Effort, Expectation, and Satisfaction," *Journal of Marketing Research* (2:3), pp. 244–249.
- Carrascal, J. P., Riederer, C., and Oliveira, R. De. 2013. "Your Browsing Behavior for a Big Mac: Economics of Personal Information Online Categories and Subject Descriptors," in *Proceedings of the 22nd International Conference on World Wide Web*, pp. 189–199.
- Carrier, L. M., Spradlin, A., Bunce, J. P., and Rosen, L. D. 2015. "Virtual Empathy: Positive and Negative Impacts of Going Online upon Empathy in Young Adults," *Computers in Human Behavior* (52), Elsevier Ltd, pp. 39–48.
- Caviola, L., Faulmüller, N., Everett, J. A. C., Savulescu, J., and Kahane, G. 2014. "The Evaluability Bias in Charitable Giving: Saving Administration Costs or Saving Lives?," *Judgment and Decision Making* (9:4), pp. 303–315.
- Cenfetelli, R. T. 2004. "Inhibitors and Enablers as Dual Factor Concepts in Technology Usage," *Journal of the Association for Information Systems* (5:11), pp. 472–492.
- Cenfetelli, R. T., and Schwarz, A. 2011. "Identifying and Testing the Inhibitors of Technology Usage Intentions," *Information Systems Research* (22:4), pp. 808–823.
- Chang, C. W., and Chen, G. M. 2014. "College Students' Disclosure of Location-Related Information on Facebook," *Computers in Human Behavior* (35), pp. 33–38.
- Chang, C. W., and Heo, J. 2014. "Visiting Theories That Predict College Students' Self-Disclosure on Facebook," *Computers in Human Behavior* (30), pp. 79–86.
- Chang, L., and Chen, J. V. 2014. "Aligning Principal and Agent's Incentives: A Principal-Agent Perspective of Social Networking Sites," *Expert Systems with Applications* (41:6), pp. 3091–3104.

- Chang, Y. W., and Chang, Y. H. 2010. "Does Service Recovery Affect Satisfaction and Customer Loyalty? An Empirical Study of Airline Services," *Journal of Air Transport Management* (16:6), pp. 340–342.
- Chelappa, R. K., and Sin, R. G. 2005. "Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management* (6), pp. 181–202.
- Chen, C. W., and Koufaris, M. 2015. "The Impact of Decision Support System Features on User Overconfidence and Risky Behavior," *European Journal of Information Systems* (24:6), Nature Publishing Group, pp. 607–623.
- Chen, J. V., Widjaja, A. E., and Yen, D. C. 2015. "Need for Affiliation, Need for Popularity, Self-Esteem, and the Moderating Effect of Big Five Personality Traits Affecting Individuals' Self-Disclosure on Facebook," *International Journal of Human-Computer Interaction* (31:11), pp. 815–831.
- Chen, R., and Sharma, S. K. 2013. "Self-Disclosure at Social Networking Sites: An Exploration through Relational Capitals," *Information Systems Frontiers* (15:2), pp. 269–278.
- Chen, X., Pan, Y., and Guo, B. 2016. "The Influence of Personality Traits and Social Networks on the Self-Disclosure Behavior of Social Network Site Users," *Internet Research* (26:3), pp. 566–586.
- Chen, Y.-T., and Chou, T.-Y. 2012. "Exploring the Continuance Intentions of Consumers for B2C Online Shopping: Perspectives of Fairness and Trust," *Online Information Review* (36:1), Emerald, pp. 104–125.
- Chennamaneni, A., and Taneja, A. 2015. "Communication Privacy Management and Self-Disclosure on Social Media - A Case of Facebook," in *Proceedings of the 21st Americas Conference on Information Systems*, pp. 1–11.
- Cheon, Y. joon, Choi, S. K., Kim, J., and Kwak, K. T. 2015. "Antecedents of Relational Inertia and Information Sharing in SNS Usage: The Moderating Role of Structural Autonomy," *Technological Forecasting and Social Change* (95), pp. 32–47.
- Cheung, C. M. K., Lee, Z. W. Y., and Chan, T. K. H. 2015. "Self-Disclosure in Social Networking Sites: The Role of Perceived Cost, Perceived Benefits and Social Influence," *Information Research* (25:2), pp. 279–300.
- Cheung, C. M. K., and Lee, M. K. O. 2006. "Understanding Consumer Trust in Internet Shopping: A Multidisciplinary Approach," *Journal of the American Society for Information Science and Technology* (57:4), pp. 479–492.
- Chin, W. W. 2010. "How to Write Up and Report PLS Analyses," in *Handbook of Partial Least Squares: Concepts, Methods and Applications*, V. E. Vinzi, W. W. Chin, J. Henseler, and H. Wang (eds.), Berlin Heidelberg: Springer, pp. 655–690.
- Chiu, C.-M., Lin, H.-Y., Sun, S.-Y., and Hsu, M.-H. 2009. "Understanding Customers' Loyalty Intentions Towards Online Shopping: An Integration of Technology Acceptance Model and Fairness Theory," *Behaviour and Information Technology* (28:4), pp. 347–360.
- Chiu, C., and Huang, H. 2014. "Examining the Antecedents of User Gratification and Its Effects on Individuals' Social Network Services Usage: The Moderating Role of Habit," *European Journal of Information Systems* (24:4), pp. 411–430.
- Chiu, C. M., Chiu, C. S., and Chang, H. C. 2007. "Examining the Integrated Influence of Fairness and Quality on Learners' Satisfaction and Web-Based Learning Continuance Intention," *Information Systems Journal* (17:3), pp. 271–287.

- Cho, H., Lee, J. S., and Chung, S. 2010. "Optimistic Bias About Online Privacy Risks: Testing the Moderating Effects of Perceived Controllability and Prior Experience," *Computers in Human Behavior* (26:5), Elsevier Ltd, pp. 987–995.
- Choi, Y. H., and Bazarova, N. N. 2020. "Self-Disclosure and Self-Presentation," *The International Encyclopedia of Media Psychology*, pp. 1–5.
- Chou, E. Y., Lin, C. Y., and Huang, H. C. 2016. "Fairness and Devotion Go Far: Integrating Online Justice and Value Co-Creation in Virtual Communities," *International Journal of Information Management* (36:1), pp. 60–72.
- Christin, D., Christian, B., and Leibecke, N. 2013. "What's the Value of Your Privacy? Exploring Factors That Influence Privacy-Sensitive Contributions to Participatory Sensing Applications," in *Proceedings of the 38th Conference on Local Computer Networks Workshops*, IEEE, pp. 918–923.
- Christofides, E., Muise, A., and Desmarais, S. 2009. "Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes?," *Cyberpsychology & Behavior: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society* (12:3), pp. 341–345.
- Christofides, E., Muise, A., and Desmarais, S. 2012. "Risky Disclosures on Facebook: The Effect of Having a Bad Experience on Online Behavior," *Journal of Adolescent Research* (27), pp. 714–731.
- Cialdini, R. B., Brown, S. L., Lewis, B. P., Luce, C., and Neuberg, S. L. 1997. "Reinterpreting the Empathy–Altruism Relationship: When One Into One Equals Oneness," *Journal of Personality and Social Psychology* (73:3), pp. 481–494.
- CIGI. 2019. "2019 CIGI-Ipsos Global Survey on Internet Security and Trust," *Center for International Governance Innovation*. (<https://www.cigionline.org/internet-survey-2019>, accessed July 6, 2020).
- Clemons, E. K. 2009. "The Complex Problem of Monetizing Virtual Electronic Social Networks," *Decision Support Systems* (48:1), pp. 46–56.
- CNBC. 2018. "Yahoo's EU Regulator Orders Privacy Changes Over Data Breach." (<https://www.cnn.com/2018/06/07/reuters-america-yahoos-eu-regulator-orders-privacy-changes-over-data-breach.html>).
- Cohen-Charash, Y. 2009. "Episodic Envy," *Journal of Applied Social Psychology* (39:9), pp. 2128–2173.
- Cohen, J. 1977. *Statistical Power Analysis for the Behavioral Sciences*, New York: Academic Press.
- comScore. 2016. "The 2016 U.S. Mobile App Report."
- Cooney, G., Gilbert, D. T., and Wilson, T. D. 2015. "Corrigendum: The Unforeseen Costs of Extraordinary Experience," *Psychological Science* (26:4), pp. 554–554.
- Creyer, E. H., and Ross, W. T. J. 1997. "Tradeoffs Between Price and Quality: How a Value Index Affects Preference Formation," *Journal of Consumer Affairs* (31:2), pp. 280–302.
- Cropanzano, R. 2005. "Social Exchange Theory: An Interdisciplinary Review," *Journal of Management* (31:6), pp. 874–900.
- Cross, T. L., Coleman, L. J., and Terhaar-yonkers, M. 1991. "The Social Cognition of Gifted Adolescents in Schools : Managing the Stigma of Giftedness," *Journal for the Education of the Gifted* (15:1), pp. 44–55.

- Culnan, M. J. 1993. "'How Did They Get My Name?': An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use," *MIS Quarterly* (September), pp. 341–364.
- Culnan, M. J. 1995. "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing," *Journal of Interactive Marketing* (9:2), pp. 10–19.
- Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104–115.
- Culnan, M. J., and Bies, J. R. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2), pp. 323–342.
- Cvrcek, D., Matyas, V., Kumpost, M., and Danezis, G. 2006. "The Value of Location Information," in *Proceedings of the ACM Workshop on Privacy in the Electronic Society*, pp. 109–118.
- Danezis, G., Lewis, S., and Anderson, R. 2005. "How Much Is Location Privacy Worth?," in *Proceedings of the 4th Workshop on the Economics of Information Security*.
- Darrat, A. A., Darrat, M. A., and Amyx, D. 2016. "How Impulse Buying Influences Compulsive Buying: The Central Role of Consumer Anxiety and Escapism," *Journal of Retailing and Consumer Services* (31), pp. 103–108.
- Das, S., and Kramer, A. 2005. "Self-Censorship on Facebook," in *Proceedings of the Seventh International AAAI Conference on Weblogs and Social Media* . (Vol. 180), pp. 120–127.
- Datacoup. 2019. "Datacoup - Unlock the Value of Your Personal Data." (<https://datacoup.com/docs#how-it-works>).
- Datawallet. 2019. "Datawallet - Take Control of Your Data." (<https://datawallet.com/home#>).
- Dauda, S. Y., and Lee, J. 2015. "Technology Adoption: A Conjoint Analysis of Consumers' Preference on Future Online Banking Services," *Information Systems* (53), Elsevier Ltd, pp. 1–15.
- Davison, A. C., and Hinkley, D. V. 1997. "Bootstrap Methods and Their Application."
- Denti, L., Barbopoulos, I., Nilsson, I., Holmberg, L., Thulin, M., Wendeblad, M., Andén, L., and Davidsson, E. 2012. "Sweden's Largest Facebook Study."
- Derlega, V., Metts, S., and Sandra, P. 1993. "Self-Disclosure," *Thousand Oaks*.
- Dinev, T. 2014. "Why Would We Care About Privacy?," *European Journal of Information Systems* (23:2), pp. 97–102.
- Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C. 2006. "Privacy Calculus Model in E-Commerce - A Study of Italy and the United States," *European Journal of Information Systems* (15), pp. 389–402.
- Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61–80.
- Dinev, T., McConnell, A. R., and Smith, H. J. 2015. "Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the 'APCO' Box," *Information Systems Research* (26:4), pp. 639–655.
- Dommeyer, C. J., and Gross, B. L. 2003. "What Consumers Know and What They Do: An Investigation of Consumer Knowledge, Awareness, and Use of Privacy Protection Strategies," *Journal of Interactive Marketing* (17:2), pp. 34–51.

- Dunning, D., Van Boven, L., and Loewenstein, G. F. 2001. "Egocentric Empathy Gaps in Social Interaction and Exchange," *Advances in Group Processes* (18), pp. 65–97.
- Egelman, S., Felt, A. P., and Wagner, D. 2012. "Choice Architecture and Smartphone Privacy: There's A Price for That," *The Economics of Information Security and Privacy*, Berlin Heidelberg: Springer.
- Egelman, S., Tsai, J., Cranor, L. F., and Acquisti, A. 2009. "Timing Is Everything? The Effects of Timing and Placement of Online Privacy Indicators," in *Proceedings of the 27th International Conference on Human Factors in Computing Systems*.
- Ehrlinger, J., Johnson, K., Banner, M., Dunning, D., and Kruger, J. 2008. "Why the Unskilled Are Unaware: Further Explorations of (Absent) Self-Insight Among the Incompetent," *Organizational Behavior and Human Decision Processes* (105:1), pp. 98–121.
- Eling, N., Büchner, C., and Buxmann, P. 2016. "Business Models for Free Digital Goods and Services," in *Proceedings of the 49th Hawaii International Conference on System Sciences*.
- Ellison, N. B., Steinfield, C., and Lampe, C. 2007. "The Benefits of Facebook 'Friends': Social Capital and College Students' Use of Online Social Network Sites," *Journal of Computer-Mediated Communication* (12:4), pp. 1143–1168.
- Ellison, N., Heino, R., and Gibbs, J. L. 2006. "Managing Impressions Online: Self-Presentation Processes in the Online Dating Environment," *Journal of Computer-Mediated Communication* (11), pp. 415–441.
- El Emam, K., Jonker, E., Arbuckle, L., and Malin, B. 2011. "A Systematic Review of Re-Identification Attacks on Health Data," *PLoS ONE* (6:12), Public Library of Science.
- Engelbrecht, A., Gerlach, J. P., and Widjaja, T. 2016. "Data-Driven Business Models – Towards an Empirical Taxonomy," in *24th European Conference on Information Systems*.
- Epley, N., Keysar, B., Van Boven, L., and Gilovich, T. 2004. "Perspective Taking as Egocentric Anchoring and Adjustment," *Journal of Personality and Social Psychology* (87:3), pp. 327–339.
- European Union Agency for Cybersecurity. 2018. "The Value of Personal Online Data," *ENISA*. (<https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data>).
- Eurostat. 2018. "Internet Access and Use Statistics - Households and Individuals." (http://ec.europa.eu/eurostat/statistics-explained/index.php/Internet_access_and_use_statistics_-_households_and_individuals).
- Evans, K. R., Schlacter, J. L., Schultz, R. J., Gremler, D. D., Pass, M., and Wolfe, W. G. 2003. "Salesperson and Sales Manager Perceptions of Salesperson Job Characteristics and Job Outcomes: A Perceptual Congruence Approach," *Journal of Marketing Theory and Practice* (10:4), pp. 1–44.
- Exline, J. J., and Lobel, M. 1999. "The Perils of Outperformance: Sensitivity About Being the Target of a Threatening Upward Comparison," *Psychological Bulletin* (125:3), pp. 307–337.
- Exline, J. J., Single, P. B., Lobel, M., and Geyer, A. 2004. "Glowing Praise and the Envious Gaze: Social Dilemmas Surrounding the Public Recognition of Achievement," *Basic and Applied Social Psychology* (26:2), pp. 119–130.

- Facebook. 2019. "Facebook Q4 2018 Results." (https://s21.q4cdn.com/399680738/files/doc_financials/2018/Q4/Q4-2018-Earnings-Presentation.pdf).
- Facebook. 2021. "Your Privacy." (https://www.facebook.com/help/238318146535333?helpref=popular_topics, accessed April 1, 2021).
- Falk, R. F., and Miller, N. B. 1992. *A Primer for Soft Modeling*, Akron, OH: University of Akron Press.
- Featherman, M. S., and Pavlou, P. A. 2003. "Predicting E-Services Adoption: A Perceived Risk Facets Perspective," *International Journal of Human Computer Studies* (59:4), pp. 451–474.
- Feijóo, C., Gómez-Barroso, J. L., and Voigt, P. 2014. "Exploring the Economic Value of Personal Information From Firms' Financial Statements," *International Journal of Information Management* (34:2), Elsevier Ltd, pp. 248–256.
- Finch, J. 1987. "The Vignette Technique in Survey Research," *Sociology* (21:1), British Sociological Association, pp. 105–114.
- Fingerman, K. L. 1995. "Aging Mothers' and Their Adult Daughters' Perceptions of Conflict Behaviors," *Psychology and Aging* (10:4), pp. 639–649.
- Fisk, R. P., and Coney, K. A. 1982. "Postchoice Evaluation: An Equity Theory Analysis of Consumer Satisfaction/Dissatisfaction with Service Choices," *Conceptual and Empirical Contributions to Consumer Satisfaction and Complaining Behavior*, pp. 9–16.
- Flavián, C., and Guinalíu, M. 2006. "Consumer Trust, Perceived Security and Privacy Policy: Three Basic Elements of Loyalty to a Web Site," *Industrial Management & Data Systems* (106:5), Emerald Group Publishing Limited, pp. 601–620.
- Fogel, J., and Nehmad, E. 2009. "Internet Social Network Communities: Risk Taking, Trust, and Privacy Concerns," *Computers in Human Behavior* (25:1), Elsevier Ltd, pp. 153–160.
- Fornell, C., and Bookstein, F. L. 1982. "Two Structural Equation Models: LISREL and PLS Applied to Consumer Exit-Voice Theory," *Journal of Marketing Research* (19:4), American Marketing Association, pp. 440–452.
- Fornell, C., and Larcker, D. F. 1981. "Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics," *Journal of Marketing Research* (18:3), American Marketing Association, pp. 382–388.
- Fortes, N., and Rita, P. 2016. "Privacy Concerns and Online Purchasing Behaviour: Towards an Integrated Model," *European Research on Management and Business Economics* (22:3), European Academy of Management and Business Economics, pp. 167–176.
- Foster, G. 1972. "The Anatomy of Envy: A Study in Symbolic Behavior," *Current Anthropology* (13), pp. 165–202.
- Fox, J., and Moreland, J. J. 2015. "The Dark Side of Social Networking Sites: An Exploration of the Relational and Psychological Stressors Associated with Facebook Use and Affordances," *Computers in Human Behavior* (45), pp. 168–176.
- Fox, J., and Rooney, M. C. 2015. "The Dark Triad and Trait Self-Objectification as Predictors of Men's Use and Self-Presentation Behaviors on Social Networking Sites," *Personality and Individual Differences* (76), Elsevier Ltd, pp. 161–165.

- Franke, N., Keinz, P., and Klausberger, K. 2013. "Does This Sound Like a Fair Deal?": Antecedents and Consequences of Fairness Expectations in the Individual's Decision to Participate in Firm Innovation," *Organization Science* (24:5), pp. 1495–1516.
- French, A. M., and Read, A. 2013. "My Mom's on Facebook: An Evaluation of Information Sharing Depth in Social Networking," *Behaviour and Information Technology* (32:10), pp. 1049–1059.
- Frey, B. S., and Pommerchne, W. W. 1991. "On the Fairness of Pricing - An Empirical Survey Among the General Population," *Journal of Economic Behavior and Organization* (20:3), pp. 295–307.
- Frison, E., and Eggermont, S. 2016. "'Harder, Better, Faster, Stronger': Negative Comparison on Facebook and Adolescents' Life Satisfaction Are Reciprocally Related," *Cyberpsychology, Behavior, and Social Networking* (19:3), pp. 158–164.
- Galinsky, A. D., Maddux, W. W., Gilin, D., and White, J. B. 2008. "Why It Pays to Get inside the Head of Your Opponent: The Differential Effects of Perspective Taking and Empathy in Negotiations: Research Article," *Psychological Science* (19:4), pp. 378–384.
- Gates, B. 1996. "Content Is King." (<http://web.archive.org/web/20010126005200/http://www.microsoft.com/billgates/columns/1996essay/essay960103.asp>).
- Gefen, D., Straub, D., and Boudreau, M. C. 2000. "Structural Equation Modeling and Regression: Guidelines for Research Practice," *Communications of the Association for Information Systems* (4:1), p. 7.
- Gerlach, J. P., Buxmann, P., and Dinev, T. 2019. "'They're All the Same!' Stereotypical Thinking and Systematic Errors in Users' Privacy-Related Judgments About Online Services," *Journal of the Association for Information Systems* (20:6), pp. 787–823.
- Gerlach, J. P., Widjaja, T., and Buxmann, P. 2015. "Handle With Care: How Online Social Network Providers' Privacy Policies Impact Users' Information Sharing Behavior," *The Journal of Strategic Information Systems* (24:1), pp. 33–43.
- Gino, F., Sharek, Z., and Moore, D. A. 2011. "Keeping the Illusion of Control under Control: Ceilings, Floors, and Imperfect Calibration," *Organizational Behavior and Human Decision Processes* (114:2), Elsevier Inc., pp. 104–114.
- Glaser, M., Langer, T., and Weber, M. 2013. "True Overconfidence in Interval Estimates: Evidence Based on a New Measure of Miscalibration," *Journal of Behavioral Decision Making* (26), pp. 405–417.
- Glaser, M., and Weber, M. 2007. "Overconfidence and Trading Volume," *GENEVA Risk and Insurance Review* (32:1), pp. 1–36.
- Goel, L., Johnson, N. A., Junglas, I., and Ives, B. 2011. "From Space to Place: Predicting Users' Intentions to Return to Virtual Worlds," *MIS Quarterly* (35:3), pp. 749–771.
- Goffman, E. 1975. "The Presentation of Self in Everyday Life," *Life as Theater*, p. 173.
- Gong, W., Lim, E.-P., and Zhu, F. 2016. "Posting Topics ≠ Reading Topics: On Discovering Posting and Reading Topics in Social Media," in *International Conference and School on Network Science*, Springer, Cham, pp. 14–28.

- Gonzales, A. L., and Hancock, J. T. 2011. "Mirror, Mirror on My Facebook Wall: Effects of Exposure to Facebook on Self-Esteem," *Cyberpsychology, Behavior, and Social Networking* (14:1–2), pp. 79–83.
- González-Vallejo, C., and Moran, E. 2001. "The Evaluability Hypothesis Revisited: Joint and Separate Evaluation Preference Reversal as a Function of Attribute Importance," *Organizational Behavior and Human Decision Processes* (86:2), Academic Press Inc., pp. 216–233.
- Green, P. E., and Krieger, A. M. 1991. "Segmenting Markets with Conjoint Analysis," *Journal of Marketing* (55:4), SAGE Publications, p. 20.
- Green, P. E., Krieger, A. M., and Wind, Y. 2001. "Thirty Years of Conjoint Analysis: Reflections and Prospects," *Interfaces* (31:3_supplement), Institute for Operations Research and the Management Sciences (INFORMS), pp. S56–S73.
- Green, P. E., and Srinivasan, V. 1978. "Conjoint Analysis in Consumer Research: Issues and Outlook," *Journal of Consumer Research* (5:2), Oxford University Press (OUP), p. 103.
- Grimaldi, P., Lau, H., and Basso, M. A. 2015. "There Are Things That We Know That We Know, And There Are Things That We Do Not Know We Do Not Know: Confidence in Decision-Making," *Neuroscience and Biobehavioral Reviews* (55), Elsevier Ltd, pp. 88–97.
- Grossklags, J., and Acquisti, A. 2007. "When 25 Cents Is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information," in *Proceedings of Workshop on the Economics of Information Security*.
- Gupta, A., and Dhami, A. 2015. "Measuring the Impact of Security, Trust and Privacy in Information Sharing: A Study on Social Networking Sites," *Journal of Direct, Data and Digital Marketing Practice* (17:1), pp. 43–53.
- Haberer, B., and Schnurr, D. 2018. "An Economic Analysis of Data Portability and Personal Data Markets," in *Proceedings of the International Conference on Information Systems*.
- Hair, J. F., Hult, G. T. M., Ringle, C., and Sarstedt, M. 2014. *A Primer on Partial Least Squares Structural Equation Modeling*, Los Angeles: Sage Publications Inc.
- Hair, J. F., Ringle, C. M., and Sarstedt, M. 2011. "PLS-SEM: Indeed a Silver Bullet," *Journal of Marketing Theory and Practice* (19:2), pp. 139–152.
- Hair, J. F., Sarstedt, M., Pieper, T. M., and Ringle, C. M. 2012. "The Use of Partial Least Squares Structural Equation Modeling in Strategic Management Research: A Review of Past Practices and Recommendations for Future Applications," *Long Range Planning* (45:5–6), Elsevier Ltd, pp. 320–340.
- Hair, J. F., Sarstedt, M., Ringle, C., and Gudergan, S. 2017. *Advanced Issues in Partial Least Squares Structural Equation Modeling*, SAGE Publications.
- Hair, J. J. F., Hult, G. T. M., Ringle, C., and Sarstedt, M. 2013. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, Sage Publications.
- Hajli, N., and Lin, X. 2016. "Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information," *Journal of Business Ethics* (133:1), pp. 111–123.
- Haley, S. M., and Osberg, J. S. 1989. "Kappa Coefficient Calculation Using Multiple Ratings Per Subject: A Special Communication," *Physical Therapy* (69:11), pp. 970–974.

- Hancock, J. T., and Toma, C. L. 2009. "Putting Your Best Face Forward: The Accuracy of Online Dating Photographs," *Journal of Communication* (59:2), pp. 367–386.
- Hann, I.-H., Hui, K.-L., Tom L., S.-Y., and Png, I. P. L. 2007. "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," *Journal of Management Information Systems* (24:2), pp. 13–42.
- Hann, I., and Lee, T. S. 2002. "Online Information Privacy: Measuring The Cost-Benefit," in *Proceedings of the 23rd International Conference on Information Systems*.
- Heath, C., and Tversky, A. 1991. "Preference and Belief: Ambiguity and Competence in Choice under Uncertainty," *Journal of Risk and Uncertainty* (4:5), pp. 5–28.
- Hedges, L., and Olkin, I. 1985. *Statistical Methods for Meta-Analysis*, (Academic P.), New York.
- Heimbach, I., Gottschlich, J., and Hinz, O. 2015. "The Value of User's Facebook Profile Data for Product Recommendation Generation," *Electronic Markets* (25:2), pp. 125–138.
- Henseler, J. 2012. "PLS-MGA: A Non-Parametric Approach to Partial Least Squares-Based Multi-Group Analysis," in *Challenges at the Interface of Data Analysis, Computer Science, and Optimization*, Springer (ed.), Kluwer Academic Publishers, pp. 495–501.
- Hensher, D. A. 1994. "Stated Preference Analysis of Travel Choices: The State of Practice," *Transportation* (21:2), Kluwer Academic Publishers, pp. 107–133.
- Herrmann, A., Xia, L., Monroe, K. B., and Huber, F. 2007. "The Influence of Price Fairness on Customer Satisfaction: An Empirical Test in the Context of Automobile Purchases," *Journal of Product & Brand Management* (16:1), pp. 49–58.
- Hilton, D., Régner, I., Cabantous, L., Charalambides, L., and Vautier, S. 2011. "Do Positive Illusions Predict Overconfidence in Judgment? A Test Using Interval Production and Probability Evaluation Measures of Miscalibration," *Journal of Behavioral Decision Making* (24:2), pp. 117–139.
- Hinkin, T., and Tracey, J. B. 1999. "An Analysis of Variance Approach to Content Validation," *Organizational Research Methods* (2:2), pp. 175–186.
- Hollenbaugh, E. E., and Ferris, A. L. 2014. "Facebook Self-Disclosure: Examining the Role of Traits, Social Cohesion, and Motives," *Computers in Human Behavior* (30), Elsevier Ltd, pp. 50–58.
- Hollenbaugh, E. E., and Ferris, A. L. 2015. "Predictors of Honesty, Intent, and Valence of Facebook Self-Disclosure," *Computers in Human Behavior* (50), pp. 456–464.
- Homans, G. 1958. "Social Behavior as Exchange," *American Journal of Sociology*, (63:6), pp. 597–606.
- Hooi, R., and Cho, H. 2013. "The Virtual 'Me' Is the Actual Me: Self-Disclosure in Virtual Environment," in *Proceedings of the 46th Hawaii International Conference on System Sciences*, pp. 883–892.
- Hsee, C. K. 2000. "Attribute Evaluability and Its Implications for Joint-Separate Evaluation Reversals and Beyond," in *CHOICES, VALUES AND FRAMES*, E. D. Kahneman & A. Tversky (ed.), Cambridge University Press.
- Hsee, C. K., Blount, S., Loewenstein, G. F., and Bazerman, M. H. 1999. "Preference Reversals Between Joint and Separate Evaluations of Options: A Review and Theoretical Analysis," *Psychological Bulletin* (125:5), American Psychological Association Inc., pp. 576–590.

- Hsee, C. K., Hsee, and K., C. 1996. "The Evaluability Hypothesis: An Explanation for Preference Reversals between Joint and Separate Evaluations of Alternatives," *Organizational Behavior and Human Decision Processes* (67:3), Elsevier, pp. 247–257.
- Hsee, C. K., and Zhang, J. 2010. "General Evaluability Theory," *Perspectives on Psychological Science* (5:4), pp. 343–355.
- Hu, H. F., Moore, W. L., and Hu, P. J. 2012. "Incorporating User Perceptions and Product Attributes in Software Product Design and Evaluation," in *Proceedings of the International Conference on Information Systems*, , December.
- Hu, L., and Bentler, P. M. 1999. "Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives," *Structural Equation Modeling: A Multidisciplinary Journal* (6:1), pp. 1–55.
- Hu, T., Kettinger, W. J., and Poston, R. S. 2015. "The Effect of Online Social Value on Satisfaction and Continued Use of Social Media," *European Journal of Information Systems* (24:4), pp. 391–410.
- Hu, Y., Manikonda, L., and Kambhampati, S. 2014. "What We Instagram: A First Analysis of Instagram Photo Content and User Types," in *Proceedings of the Eight International AAAI Conference on Weblogs and Social Media*, pp. 595–598.
- Huang, L.-T., Farn, C., and Yin, K.-L. 2005. "On Initial Trust Building for E-Commerce: Revisiting from the Perspective of Signal Theory and Trust Transference," in *Proceedings of the European Conference on Information Systems*.
- Huberman, B. A., Adar, E., Fine, L. R., Labs, H. P., Road, P. M., and Ca, P. A. 2005. "Valuating Privacy," *IEEE Security & Privacy* (3:5), pp. 22–25.
- Hulland, J. 1999. "Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies," *Strategic Management Journal* (20:2), pp. 195–204.
- Huppertz, J. W. 1979. "Measuring Cotnponents of Equity in the Marketplace: Perceptions of Inputs and Outcomes by Satisfied and Dissatisfied Consumers," *New Dimensions of Consumer Satisfaction and Complaining Behavior*.
- Internet live Stats. 2020. "Google Search Statistics." (<https://www.internetlivestats.com/google-search-statistics/>, accessed August 12, 2020).
- Iyer, G., Soberman, D., and Villas-Boas, J. M. 2005. "The Targeting of Advertising," *Marketing Science* (24:3), pp. 461–476.
- James, T. L., Lowry, P. B., Wallace, L., and Warkentin, M. 2017. "The Effect of Belongingness on Obsessive-Compulsive Disorder in the Use of Online Social Networks," *Journal of Management Information Systems* (34:2), pp. 560–596.
- Jensen, Carlos, Potts, C., and Jensen, Christian. 2005. "Privacy Practices of Internet Users: Self-Reports versus Observed Behavior," *International Journal of Human Computer Studies* (63:1–2), pp. 203–227. (<https://doi.org/10.1016/j.ijhcs.2005.04.019>).
- Jentzsch, N. 2014. "Auctioning Privacy-Sensitive Goods: A Note on Incentive-Compatibility," in *Privacy Technologies and Policy*, Cham: Springer, pp. 133–142.
- Jia, Y., Zhao, Y., and Lin, Y. 2010. "Effects of System Characteristics on Users' Self-Disclosure in Social Networking Sites," in *Proceedings of the 7th International Conference on Information Technology: New Generations*, pp. 529–533.

- Jiang, L. C., Bazarova, N. N., and Hancock, J. T. 2011. "The Disclosure-Intimacy Link in Computer-Mediated Communication: An Attributional Extension of the Hyperpersonal Model," *Human Communication Research* (37:1), pp. 58–77.
- John, L. K., Acquisti, A., and Loewenstein, G. 2011. "The Best of Strangers: Context-Dependent Willingness to Divulge Personal Information," *The Journal of Consumer Research* (37), pp. 858–873.
- Johnson, J. A. 2005. "Ascertaining the Validity of Individual Protocols from Web-Based Personality Inventories," *Journal of Research in Personality* (39:1 SPEC. ISS.), Academic Press Inc., pp. 103–129.
- Johnson, R. M. 1974. "Trade-off Analysis of Consumer Values," *Journal of Marketing Research* (11:2), JSTOR, p. 121.
- Johnston, K., Tanner, M., Lalla, N., and Kawalski, D. 2011. "Social Capital: The Benefit of Facebook Friends," *Behaviour & Information Technology* (32:1), pp. 1–13.
- Joinson, A. N., and Paine, C. B. 2007. "Self-Disclosure, Privacy and the Internet," in *Oxford Handbook of Internet Psychology - Google Books*, pp. 237–251.
- Joinson, A. N., Woodley, A., and Reips, U. D. 2007. "Personalization, Authentication and Self-Disclosure in Self-Administered Internet Surveys," *Computers in Human Behavior* (23:1), Pergamon, pp. 275–285.
- Joshi, K. 1989. "The Measurement of Fairness or Equity Perceptions of Management Information Systems Users," *MIS Quarterly* (13:3), p. 343.
- Jourard, S. M., and Lasakow, P. 1958. "Some Factors in Self-Disclosure," *Journal of Abnormal and Social Psychology* (56:1), pp. 91–98.
- Kahneman, D., Slovic, P., and Tversky, A. 1982. *Judgment Under Uncertainty: Heuristics and Biases*, New York: Cambridge University Press.
- Kamleitner, B., and Haddadi, H. 2016. "Can Users Price Real-Time Contextual Information?," in *ACM Transactions on Internet Technology. Special Issue on Economics of Security and Privacy*.
- Kane, Gerald C., Alavi, M., Labianca, G. J., and Borgatti, S. 2014. "What's Different About Social Media Networks? A Framework and Research Agenda," *MIS Quarterly* (38:1), pp. 274–304.
- Kannan, K. S., Manoj, K., and Arumugam, S. 2015. "Labeling Methods for Identifying Outliers," *International Journal of Statistics and Systems* (10:2), pp. 231–238.
- Karniouchina, E. V., Moore, W. L., van der Rhee, B., and Verma, R. 2009. "Issues in the Use of Ratings-Based versus Choice-Based Conjoint Analysis in Operations Management Research," *European Journal of Operational Research* (197:1), pp. 340–348.
- Kaura, V., Prasad, C. S. D., and Sharma, S. 2015. "Service Quality, Service Convenience, Price and Fairness, Customer Loyalty, and the Mediating Role of Customer Satisfaction," *International Journal of Bank Marketing* (33:4), Emerald Group Publishing Ltd., pp. 404–422.
- Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. 2015. "Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus," *Information Systems Journal* (25:6), pp. 607–635.

- Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., and Greer, C. 2013. "Information Disclosure on Mobile Devices: Re-Examining Privacy Calculus with Actual User Behavior," *International Journal of Human Computer Studies* (71:12), Academic Press, pp. 1163–1173.
- Keith, M., Thompson, S. C., Hale, J. E., and Greer, C. 2012. "Examining the Rationality of Information Disclosure through Mobile Devices," in *Proceedings of the 33rd International Conference on Information Systems*.
- Kelley, H. H. 1973. "The Processes of Causal Attribution.," *American Psychologist* (28:2), American Psychological Association (APA), pp. 107–128.
- Kelley, P. G., Cranor, L. F., and Sadeh, N. 2013. "Privacy as Part of the App Decision-Making Process," in *Proceedings of the Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, pp. 3393–3402.
- de Kerviler, G., Demoulin, N. T. M., and Zidda, P. 2016. "Adoption of In-Store Mobile Payment: Are Perceived Risk and Convenience the Only Drivers?," *Journal of Retailing and Consumer Services* (31), Elsevier Ltd, pp. 334–344.
- Kesharwani, A., and Bisht, S. S. 2012. "The Impact of Trust and Perceived Risk on Internet Banking Adoption in India: An Extension of Technology Acceptance Model," *International Journal of Bank Marketing* (30:4), Emerald Group Publishing Ltd., pp. 303–322.
- Kidd, R. F. 1976. "Manipulation Checks: Advantage or Disadvantage?," *Representative Research in Social Psychology* (7:2), pp. 160–165.
- Kim, E., Lee, J.-A., Sung, Y., and Choi, S. M. 2016. "Predicting Selfie-Posting Behavior On Social Networking Sites: An Extension of Theory of Planned Behavior," *Computers in Human Behavior* (62), pp. 116–123.
- Kim, J., Lee, C., and Elias, T. 2015. "Factors Affecting Information Sharing in Social Networking Sites Amongst University Students," *Online Information Review* (39:3), pp. 290–309.
- Kim, J., and Lee, J.-E. R. 2011. "The Facebook Paths to Happiness: Effects of the Number of Facebook Friends and Self-Presentation on Subjective Well-Being," *Cyberpsychology, Behavior, and Social Networking* (14:6), pp. 359–364.
- Kirk, R. 2014. "Experimental Design: Procedures for the Behavioral Sciences," *Experimental Design: Procedures for the Behavioral Sciences*, SAGE Publications, Inc.
- Klayman, J., and Gonza, C. 1999. "Overconfidence : It Depends on How, What, and Whom You Ask," *Organizational Behavior and Human Decision Processes* (79:3), pp. 216–247.
- Ko, H. C., and Chen, T. K. 2009. "Understanding the Continuous Self-Disclosure of Bloggers from the Cost-Benefit Perspective," in *Proceedings of the 2nd Conference on Human System Interactions*, pp. 520–527.
- Kokolakis, S. 2017. "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on The Privacy Paradox Phenomenon," *Computers and Security* (64), Elsevier Ltd, pp. 122–134.
- Konrath, S., O'Brien, E., and Hsing, C. 2010. "Changes in Dispositional Empathy in American College Students over Time: A Meta-Analysis. *Personality and Social Psychology*," (Vol. 15).
- Korea Bizwire. 2017. "SNS Users Weary from Information Overload."

- Korff, S., and Böhme, R. 2014. "Too Much Choice: End-User Privacy Decisions in the Context of Choice Proliferation," in *Proceedings of the Tenth Symposium On Usable Privacy and Security*, pp. 69–87.
- Koroleva, K., Krasnova, H., and Günther, O. 2011. "Cognition or Affect? - Exploring Information Processing on Facebook," in *Proceedings of International Conference on Social Informatics*, Springer Berlin Heidelberg, pp. 171–183.
- Krämer, N. C., and Winter, S. 2008. "Impression Management 2.0: The Relationship of Self-Esteem, Extraversion, Self-Efficacy, and Self-Presentation Within Social Networking Sites," *Journal of Media Psychology* (20:3), pp. 106–116.
- Krasnova, H., Abramova, O., Eling, N., and Buxmann, P. 2014. "Dangers of Facebook Login for Mobile Apps: Is There a Price Tag for Social Information?," in *Proceedings of 35th International Conference on Information Systems*.
- Krasnova, H., Günther, O., Spiekermann, S., and Koroleva, K. 2009a. "Privacy Concerns and Identity in Online Social Networks," *Identity in the Information Society* (2:1), pp. 39–63.
- Krasnova, H., Hildebrand, T., and Guenther, O. 2009b. "Investigating the Value of Privacy in Online Social Networks: Conjoint Analysis," in *Proceedings of the 30th International Conference on Information Systems*.
- Krasnova, H., and Kift, P. 2012. "Online Privacy Concerns and Legal Assurance: A User Perspective," in *Workshop on Information Security and Privacy*.
- Krasnova, H., Kolesnikova, E., and Guenther, O. 2010b. "Leveraging Trust and Privacy Concerns in Online Social Networks: An Empirical Study," in *Proceedings of the 18th European Conference on Information Systems*.
- Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. 2010a. "Online Social Networks: Why We Disclose," *Journal of Information Technology* (25:2), Routledge, pp. 109–125.
- Krasnova, H., Veltri, N. F., Eling, N., and Buxmann, P. 2017. "Why Men and Women Continue to Use Social Networking Sites: The Role of Gender Differences," *The Journal of Strategic Information Systems* (26:4), pp. 261–284.
- Krasnova, H., Veltri, N. F., and Gunther, O. 2012. "Self-Disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture: Intercultural Dynamics of Privacy Calculus," in *Proceedings of Internationale Tagung Wirtschaftsinformatik*, pp. 123–132.
- Krasnova, Hanna, Veltri, N. F., and Günther, O. 2012. "Self-Disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture Intercultural Dynamics of Privacy Calculus," *Business and Information Systems Engineering* (4:3), pp. 127–135.
- Krasnova, H., Widjaja, T., Buxmann, P., Wenninger, H., and Benbasat, I. 2015. "Why Following Friends Can Hurt You: An Networking Sites among College-Age Users College-Age Users," *Information Systems Research* (26:3), pp. 585–605.
- Kruger, J., and Dunning, D. 2002. "Unskilled and Unaware--But Why? A Reply to Krueger and Mueller (2002)," *Journal of Personality & Social Psychology* (82:2), American Psychological Association (APA), pp. 189–192.
- Kruger, J., Epley, N., Parker, J., and Ng, Z.-W. 2005. "Egocentrism Over E-Mail: Can We Communicate As Well As We Think?," *Journal of Personality and Social Psychology* (89:6), pp. 925–936.

- Kuneva, M. 2013. "European Consumer Commissioner Keynote Speech - Roundtable on Online Data Collection, Targeting and Profiling Brussels." (http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm).
- Kuo, Y.-F., and Wu, C.-M. 2011. "Satisfaction and Post-Purchase Intentions with Service Recovery of Online Shopping Websites: Perspectives on Perceived Justice and Emotions," *International Journal of Information Management* (32), pp. 127–138.
- Kwak, K. T., Choi, S. K., and Lee, B. G. 2014. "SNS Flow, SNS Self-Disclosure and Post Hoc Interpersonal Relations Change: Focused on Korean Facebook User," *Computers in Human Behavior* (31:1), Elsevier Ltd, pp. 294–304.
- Lange, J., and Crusius, J. 2015. "The Tango of Two Deadly Sins: The Social-Functional Relation of Envy and Pride," *Journal of Personality and Social Psychology* (109:3), pp. 453–472.
- Langer, E. J., Marcus, C., Roth, J., and Hall, R. 1975. "The Illusion of Control," *Social Psychology* (32:2), pp. 311–328.
- Lankton, N., McKnight, D. H., and Tripp, J. 2015. "Technology, Humanness, and Trust: Rethinking Trust in Technology," *Journal of the Association for Information Systems* (16:10), pp. 880–918.
- last10k. 2018. "Annual Report Acxiom Corporation." (https://last10k.com/sec-filings/acxm/0000733269-18-000016.htm#fullReport?utm_source=last10k&utm_medium=PDF&utm_campaign=share&utm_term=733269).
- Laudon, K. C. 1996. "Markets and Privacy," *Communications of the ACM* (39:9).
- Laudon, K. C. 1997. "Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information."
- Laufer, R. S., and Wolfe, M. 1977. "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," *Journal of Social Issues* (33:3), pp. 22–42.
- Leary, M. R. 1999. "Sense of Self-Esteem," *Current Directions in Psychological Science* 1 (8:1), pp. 32–35.
- Leary, M. R., and Kowalski, R. M. 1990. "Impression Management: A Literature Review and Two-Component Model," *Psychological Bulletin* (107:1), pp. 34–47.
- Lee, A. R., Son, S. M., and Kim, K. K. 2016. "Information and Communication Technology Overload and Social Networking Service Fatigue: A Stress Perspective," *Computers in Human Behavior* (55), Elsevier Ltd, pp. 51–61.
- Lee, E., Kim, Y. J., and Ahn, J. 2014. "How Do People Use Facebook Features to Manage Social Capital?," *Computers in Human Behavior* (36), Elsevier Ltd, pp. 440–445.
- Lee, H., Park, H., and Kim, J. 2013. "Why Do People Share Their Context Information on Social Network Services? A Qualitative Study and an Experimental Study on Users' Behavior of Balancing Perceived Benefit and Risk," *International Journal of Human Computer Studies* (71:9), Elsevier, pp. 862–877.
- Lee, M. C. 2009. "Predicting and Explaining the Adoption of Online Trading: An Empirical Study in Taiwan," *Decision Support Systems* (47:2), Elsevier Science Publishers B. V. PUB568 Amsterdam, The Netherlands, The Netherlands, pp. 133–142.

- Lee, S. Y., Hansen, S. S., and Lee, J. K. 2016. "What Makes Us Click Like on Facebook? Examining Psychological, Technological, and Motivational Factors on Virtual Endorsement," *Computer Communications* (73), pp. 332–341.
- Leith, K. P., and Baumeister, R. F. 1998. "Empathy, Shame, Guilt, and Narratives of Interpersonal Conflicts: Guilt-Prone People Are Better at Perspective Taking," *Journal of Personality* (66), pp. 1–38.
- Leventhal, G. 1980. "What Should Be Done With Equity Theory?," *Social Exchange*, pp. 27–55.
- Levinger, G., and Breedlove, J. 1966. "Interpersonal Attraction and Agreement: A Study of Marriage Partners," *Journal of Personality and Social Psychology* (3:4), pp. 367–372.
- Li, C., Li, D. Y., Miklau, G., and Suciu, D. 2014. "A Theory of Pricing Private Data," *ACM Transactions on Database Systems* (39:4), pp. 1–28.
- Li, H., Gupta, A., Zhang, J., and Sarathy, R. 2014. "Examining the Decision to Use Standalone Personal Health Record Systems as a Trust-Enabled Fair Social Contract," *Decision Support Systems* (57:1), Elsevier B.V., pp. 376–386.
- Li, H., Luo, X. (Robert), Zhang, J., and Xu, H. 2017. "Resolving the Privacy Paradox: Toward a Cognitive Appraisal and Emotion Approach to Online Privacy Behaviors," *Information and Management* (54:8), Elsevier B.V., pp. 1012–1022.
- Li, H., Wu, J., Gao, Y., and Shi, Y. 2016. "Examining Individuals' Adoption of Healthcare Wearable Devices: An Empirical Study from Privacy Calculus Perspective," *International Journal of Medical Informatics* (88), Elsevier Ireland Ltd, pp. 8–17.
- Li, K., Lin, Z., and Wang, X. 2015. "An Empirical Analysis of Users' Privacy Disclosure Behaviors on Social Network Sites," *Information and Management* (52:7), pp. 882–891.
- Li, X., and Zhang, T. 2017. "An Exploration on Artificial Intelligence Application: From Security, Privacy and Ethic Perspective," in *Proceedings of the 2nd IEEE International Conference on Cloud Computing and Big Data Analysis*, Institute of Electrical and Electronics Engineers Inc., pp. 416–420.
- Li, Y. 2012. "Theories in Online Information Privacy Research: A Critical Review and an Integrated Framework," *Decision Support Systems* (54:1), Elsevier B.V., pp. 471–481.
- Lichtenstein, D. R., and Burton, S. 1988. "The Measurement and Moderating Role of Confidence in Attributions," *ACR North American Advances* (NA-15).
- Lo, J., and Riemenschneider, C. 2010. "An Examination of Privacy Concerns and Trust Entities in Determining Willingness to Disclose Personal Information on a Social Networking Site," in *Proceedings of the 12th Americas Conference On Information Systems*.
- Loiacono, E. T. 2014. "Self-Disclosure Behavior on Social Networking Web Sites.," *International Journal of Electronic Commerce* (19:2), pp. 66–94.
- Louviere, J. J. 1988. "Conjoint Analysis Modelling of Stated Preferences: A Review of Theory, Methods, Recent Developments and External Validity on JSTOR," *Journal of Transport Economics and Policy* (22:1), pp. 93–119.
- Lowry, P. B., Moody, G., Vance, A., Jensen, M., Jenkins, J., and Wells, T. 2012. "Using an Elaboration Likelihood Approach to Better Understand the Persuasiveness of Website Privacy Assurance Cues

for Online Consumers,” *Journal of the American Society for Information Science and Technology* (63:4), pp. 755–776.

Lowry, P. B., Zhang, J., Wang, C., and Siponen, M. 2016. “Why Do Adults Engage in Cyberbullying on Social Media? An Integration of Online Disinhibition and Deindividuation Effects with the Social Structure and Social Learning Model,” *Information Systems Research* (27:4), pp. 962–986.

Lyu, S. O. 2016. “Travel Selfies on Social Media as Objectified Self-Presentation,” *Tourism Management* (54), pp. 185–195.

Ma, X., Hancock, J., and Naaman, M. 2016. “Anonymity , Intimacy and Self-Disclosure in Social Media,” in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pp. 3857–3869.

MacKenzie, S. B. 2003. “The Dangers of Poor Construct Conceptualization,” *Journal of the Academy of Marketing Science* (31:3), pp. 323–326.

MacKenzie, S. B., Podsakoff, P. M., and Podsakoff, N. P. 2011. “Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques,” *MIS Quarterly* (35:2), pp. 293–334.

Maksl, A., and Young, R. 2013a. “Affording to Exchange: Social Capital and Online Information Sharing,” *Cyberpsychology, Behavior and Social Networking* (16:8), pp. 588–92.

Malheiros, M., Brostoff, S., Jennett, C., and Sasse, M. A. 2013. “Would You Sell Your Mother’s Data? Personal Data Disclosure in a Simulated Credit Card Application,” in *The Economics of Information Security and Privacy*, Springer Berlin Heidelberg, pp. 237–261.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. “Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model,” *Information Systems Research* (15:4), pp. 336–355.

Malmendier, U., and Tate, G. 2005. “CEO Overconfidence and Corporate Investment,” *The Journal of Finance* (LX:6), pp. 2661–2700.

Margaryan, A., Littlejohn, A., and Vojt, G. 2011. “Are Digital Natives a Myth or Reality? University Students’ Use of Digital Technologies,” *Computers and Education* (56:2), pp. 429–440.

Marsden, P. V., and Campbell, K. E. 1984. “Measuring Tie Strength,” *Social Forces* (63:2), pp. 482–501.

Marshall, T. C., Lefringhausen, K., and Ferenczi, N. 2015. “The Big Five, Self-Esteem, and Narcissism as Predictors of the Topics People Write about in Facebook Status Updates,” *Personality and Individual Differences* (85), pp. 35–40.

Martinez-Tur, V., Peiro, M. J., Ramos, J., and Moliner, C. 2006. “Justice Perceptions as Predictors of Customer Satisfaction : The Impact of Distributive , Procedural , and Interactional,” *Journal of Applied Social Psychology* (1:36), pp. 100–119.

Marwick, A. E., and Boyd, D. 2011. “I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience,” *New Media and Society* (13:1), pp. 114–133.

Matzutt, R., Müllmann, D., Zeissig, E.-M., Horst, C., Kasugai, K., Lidynia, S., Wieninger, S., Ziegeldorf, J. H., Gudergan, G., Wehrle, K. 2017. “Mynedata: Towards a Trusted and User-Controlled Ecosystem for Sharing Personal Data,” *INFORMATIK*.

- McFarlin, D. B., and Sweeney, P. D. 1992. "Distributive and Procedural Justice As Predictors of Satisfaction With Personal and Organizational Outcomes," *Academy of Management Journal* (35:3), pp. 626–637.
- McKenzie, C. R. M., Liersch, M. J., and Yaniv, I. 2008. "Overconfidence in Interval Estimates: What Does Expertise Buy You?," *Organizational Behavior and Human Decision Processes* (107), pp. 179–191.
- McKnight, D. H., Lankton, N., Environment, L., and Tripp, J. 2011. "Social Networking Information Disclosure and Continuance Intention: A Disconnect," in *Proceedings of the 44th Hawaii International Conference on System Sciences*.
- Meade, A. W., and Craig, S. B. 2012. "Identifying Careless Responses in Survey Data," *Psychological Methods* (17:3), pp. 437–455.
- Mehdizadeh, S. 2010. "Self-Presentation 2.0: Narcissism and Self-Esteem on Facebook.," *Cyberpsychology, Behavior, and Social Networking* (13:4), pp. 357–64.
- Metzger, M. J. 2007. "Communication Privacy Management in Electronic Commerce," *Journal of Computer-Mediated Communication* (12:2), pp. 1–27.
- Miles, M. B., and Huberman, A. M. 1994. *Qualitative Data Analysis: An Expanded Sourcebook*, CA, US: Sage Publications: Thousands Oaks.
- Milne, G. R., Pettinico, G., Hajjat, F. M., and Markos, E. 2017. "Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing," *Journal of Consumer Affairs* (51:1), Blackwell Publishing Inc., pp. 133–161.
- Min, J. 2016. "Personal Information Concerns and Provision in Social Network Sites: Interplay Between Secure Preservation and True Presentation," *Journal of the Association for Information Science and Technology* (1:67), pp. 26–42.
- Min, J., and Kim, B. 2015. "How Are People Enticed to Disclose Personal Information Despite Privacy Concerns in Social Network Sites? The Calculus between Benefit and Cost," *Journal of the Association for Information Science and Technology* (66:4), John Wiley and Sons Inc., pp. 839–857.
- Mingers, J. 2001. "Combining IS Research Methods: Towards a Pluralist Methodology," *Information Systems Research* (12:3), INFORMS Inst.for Operations Res.and the Management Sciences, pp. 240–259.
- Mital, M., Israel, D., Agarwal, S., Colomo-Palacios, R., and Mital, M. 2010. "Information Exchange and Information Disclosure in Social Networking Web Sites: Mediating Role of Trust," *The Learning Organization* (17:6), pp. 479–490.
- Mizerski, R. W., Golden, L. L., and Kernan, J. B. 1979. "The Attribution Process in Consumer Decision Making," *Journal of Consumer Research* (6:2), Oxford University Press (OUP), p. 123.
- Moore, D. A., and Healy, P. J. 2008. "The Trouble With Overconfidence," *Psychological Review* (115:2), pp. 502–517.
- Moore, T. T., and Chang, J. C. 2009. "Self-Efficacy, Overconfidence, and the Negative Effect on Subsequent Performance: A Field Study," *Information & Management* (46), pp. 69–76.
- Moran, S., and Schweitzer, M. E. 2008. "When Better Is Worse: Envy and the Use of Deception in Negotiations," *Negotiation and Conflict Management Research* (1:1), pp. 3–29.

- Morosan, C., and DeFranco, A. 2015. "Disclosing Personal Information via Hotel Apps: A Privacy Calculus Perspective," *International Journal of Hospitality Management* (47), Elsevier Ltd, pp. 120–130.
- Morrison, R. L., and Bellack, A. S. 1981. "The Role of Social Perception in Social Skill," *Behavior Therapy* (12:1), pp. 69–79.
- Mosteller, J., and Poddar, A. 2017. "To Share and Protect: Using Regulatory Focus Theory to Examine the Privacy Paradox of Consumers' Social Media Engagement and Online Privacy Protection Behaviors," *Journal of Interactive Marketing* (39), Elsevier Inc., pp. 27–38.
- Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., and Wang, S. 2012. "Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information," *Journal of Service Research* (15:1), SAGE PublicationsSage CA: Los Angeles, pp. 76–98.
- Naaman, M., Boase, J., and Lai, C.-H. 2010. "Is It Really About Me? Message Content in Social Awareness Streams," in *Proceedings of the ACM Conference on Computer Supported Cooperative Work*.
- New York Times. 2012. *Start-Ups Seek to Help Users Put a Price on Their Personal Data*. (<http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html>).
- New York Times. 2018. "Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users." (<https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html>, accessed July 4, 2018).
- Ng, M. 2014. "Consumer Motivations to Disclose Information and Participate in Commercial Activities on Facebook," *Journal of Global Scholars of Marketing Science*, Taylor & Francis, pp. 365–383.
- Nguyen, K. D., Rosoff, H., and John, R. S. 2016. "The Effects of Attacker Identity and Individual User Characteristics on the Value of Information Privacy," *Computers in Human Behavior* (55:1), pp. 372–374.
- Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The Privacy Paradox : Personal Information Disclosure Intentions Vers Us Behaviors," *The Journal of Consumer Affairs* (41:1), pp. 100–126.
- Oh, H. J., and Larose, R. 2016. "Impression Management Concerns and Support-Seeking Behavior on Social Network Sites," *Computers in Human Behavior* (57:November), Elsevier Ltd, pp. 38–47.
- Oliver, R.L. and Swan, J. E. 1989. "Consumer Perceptions of Interpersonal Equity and Satisfaction in Transactions: A Field Survey Approach," *Journal of Marketing* (53:April), pp. 21–35.
- Olmstead, K., and Atkinson, M. 2015. "An Analysis of Apps in the Google Play Store," *Pew Research Center*. (<http://www.pewinternet.org/2015/11/10/an-analysis-of-apps-in-the-google-play-store/>).
- Omarzu, J. 2000. "A Disclosure Decision Model: Determining How and When Individuals Will Self-Disclose," *Personality and Social Psychology Review* (4:2), pp. 174–185.
- Orange. 2014. "The Future of Digital Trust - A European Study on the Nature of Consumer Trust and Personal Data."
- Orme, B. 2002. "Formulating Attributes and Levels in Conjoint Analysis," *Sawtooth Software Research Paper*, pp. 1–4.

- Oskamp, S. 1965. "Overconfidence in Case-Study Judgments," *Journal of Consulting Psychology* (29:3), pp. 261–265.
- Pan, Y., and Zinkhan, G. M. 2006. "Exploring the Impact of Online Privacy Disclosures on Consumer Trust," *Journal of Retailing* (82:4), pp. 331–338.
- Park, N., Jin, B., and Annie Jin, S. A. 2011. "Effects of Self-Disclosure on Relational Intimacy in Facebook," *Computers in Human Behavior* (27:5), pp. 1974–1983.
- Park, Y. J., and Jang, S. M. 2014. "Understanding Privacy Knowledge and Skill in Mobile Communication," *Computers in Human Behavior* (38), Elsevier Ltd, pp. 296–303.
- Parker, S. K., Axtell, C. M., and Parker, S. K. 2017. "Seeing Another Viewpoint: Antecedents and Outcomes of Employee Perspective Taking," *Academy of Management Journal* (44:6), pp. 1085–1100.
- Pavlou, P. A. 2011. "State of the Information Privacy Literature: Where Are We Now and Where Should We Go?," *MIS Quarterly* (35:4), pp. 977–988.
- Pavlou, P. A., and Fygenson, M. 2006. "Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior," *MIS Quarterly* (30:1), pp. 115–143.
- Peluchette, J., and Karl, K. 2009. "Examining Students' Intended Image on Facebook: 'What Were They Thinking?'," *Journal of Education for Business* (85:1), pp. 30–37.
- Peña, J., and Brody, N. 2014. "Intentions to Hide and Unfriend Facebook Connections Based on Perceptions of Sender Attractiveness and Status Updates," *Computers in Human Behavior* (31:1), pp. 143–150.
- Pentina, I., and Zhang, L. 2016. "Effects of Social Support and Personality on Emotional Disclosure on Facebook and in Real Life," *Behaviour & Information Technology*, pp. 1–9.
- Penttinen, E., Halme, M., Malo, P., Saarinen, T., and Vilén, V. M. 2019. "Playing for Fun or for Profit: How Extrinsically-Motivated and Intrinsically-Motivated Players Make the Choice Between Competing Dual-Purposed Gaming Platforms," *Electronic Markets* (29:3), Springer Verlag, pp. 337–358.
- Perdue, B. C., and Summers, J. O. 1986. "Checking the Success of Manipulations in Marketing Experiments," *Journal of Marketing Research* (23:4), SAGE Publications, pp. 317–326.
- Perez, S. 2017. "App Annie: Android to Top Ios in App Store Revenue This Year."
- Perusco, L., and Michael, K. 2007. "Control, Trust, Privacy, and Security: Evaluating Location-Based Services," *IEEE Technology and Society Magazine* (26:1), Institute of Electrical and Electronics Engineers Inc., pp. 4–16.
- Petty, R. E., and Cacioppo, J. T. 1986. "The Elaboration Likelihood Model of Persuasion," *Advances in Experimental Social Psychology* (19), pp. 123–205.
- Pew Research. 2016. "Social Media Update 2016." (<http://www.pewinternet.org/2016/11/11/social-media-update-2016/>).
- Phelps, J., Nowak, G., and Ferrell, E. 2000. "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy & Marketing* (19:1), pp. 27–41.
- Pinkerton, S., Tobin, J. L., Querfurth, S. C., Pena, I. M., and Wilson, K. S. 2017. "'Those Sweet, Sweet Likes': Sharing Physical Activity Over Social Network Sites," *Computers in Human Behavior* (69), Elsevier Ltd, pp. 128–135.

- Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88:5), pp. 879–903.
- Potoglou, D., Patil, S., Gijón, C., Palacios, J., and Feijóo, C. 2013. "The Value of Personal Information Online: Results from Three Stated Preference Discrete Choice Experiments in the UK," in *Proceedings of the 21st European Conference for Information Systems*.
- Preibusch, S. 2013. "The Value of Privacy in Web Search," in *The Twelfth Workshop on the Economics of Information Security (WEIS)*.
- Preibusch, S. 2015. "The Value of Web Search Privacy," *IEEE Security & Privacy* (13:5), pp. 24–32.
- Preibusch, S., Kübler, D., and Alastair R., B. 2013. "Price versus Privacy: An Experiment into the Competitive Advantage of Collecting Less Personal Information," *Electronic Commerce Research* (13:4), pp. 423–455.
- Pu, Y., and Grossklags, J. 2015. "Towards a Model on the Factors Influencing Social App Users' Valuation of Interdependent Privacy," in *Proceedings on Privacy Enhancing Technologies*.
- Qiu, L., Lin, H., Leung, A. K., and Tov, W. 2012. "Putting Their Best Foot Forward: Emotional Disclosure on Facebook," *Cyberpsychology, Behavior, and Social Networking* (15:10), pp. 569–572.
- Quan-Haase, A., and Young, A. L. 2010. "Uses and Gratifications of Social Media: A Comparison of Facebook and Instant Messaging," *Bulletin of Science, Technology & Society* (30:5), pp. 350–361.
- Qureshi, I., and Compeau, D. 2009. "Assessing Between-Group Differences in Information Systems Research: A Comparison of Covariance- and Component-Based SEM," *MIS Quarterly* (33:1), pp. 197–214.
- Racherla, P., Babb, J. S., and Keith, M. J. 2011. "Pay-What-You-Want Pricing for Mobile Applications: The Effect of Privacy Assurances and Social Information," in *Proceedings of the Conference for Information Systems Applied Research*.
- Regner, T., and Riegner, G. 2017. "Privacy Is Precious : On the Attempt to Lift Anonymity on the Internet to Increase Revenue," *Journal of Economics & Management Strategy* (26:2), pp. 318–336.
- Reynolds, C. R. 1982. "Methods for Detecting Construct and Predictive Bias," in *Handbook of Methods for Detecting Test Bias*, pp. 199–227.
- Ringle, C. M., Wende, S., and Becker, J.-M. 2015. *SmartPLS 3*, Boenningstedt: SmartPLS GmbH.
- Roeber, B., Rehse, O., Knorrek, R., and Thomsen, B. 2015. "Personal Data: How Context Shapes Consumers' Data Sharing with Organizations from Various Sectors," *Electronic Markets* (25:95), pp. 95–108.
- Rönkkö, M., and Ylitalo, J. 2011. "PLS Marker Variable Approach to Diagnosing and Controlling for Method Variance," in *Proceedings of the Thirty Second International Conference on Information Systems*.
- Rose, E. 2005. "Data Users versus Data Subjects: Are Consumers Willing to Pay for Property Rights to Personal Information?," in *Proceedings of the 38th Hawaii International Conference on System Sciences*, IEEE.
- Ross, L. 1977. "The Intuitive Psychologist and His Shortcomings: Distortion in The Attributional Process," *Advances in Experimental Social Psychology* (Vol. 10).

- Ross, L., Greene, D., and House, P. 1977. "The 'False Consensus Effect': An Egocentric Bias in Social Perception and Attribution Processes," *Journal of Experimental Social Psychology* (13:3), pp. 279–301.
- Roßnagel, H., Zibuschka, J., Hinz, O., and Muntermann, J. 2014. "Users' Willingness to Pay for Web Identity Management Systems," *European Journal of Information Systems* (23:1), Palgrave Macmillan Ltd., pp. 36–50.
- Russo, J. E., and Schoemaker, P. H. 1992. "Managing Overconfidence."
- Rust, R. T., Kannan, P. K., and Peng, N. 2002. "The Customer Economics of Internet Privacy," *Journal of the Academy of Marketing Science* (30:4), pp. 455–464.
- Ruyter, K. de, and Wetzels, M. 2000. "Customer Equity Considerations in Service Recovery: A Cross-Industry Perspective," *International Journal of Service Industry Management* (11:1), pp. 91–108.
- Ryan, G. W., and Bernard, H. R. 2000. "Data Management and Analysis Methods," in *Handbook of Qualitative Research* (2nd ed.), N. Denzin and Y. Lincoln (eds.), CA:Sage: Thousand Oaks, pp. 769–802.
- Ryan, G. W., and Bernard, H. R. 2003. "Techniques to Identify Themes," *Field Methods* (15:1), SAGE Publications, pp. 85–109.
- Ryvkin, D., Krajč, M., and Ortmann, A. 2012. "Are the Unskilled Doomed to Remain Unaware?," *Journal of Economic Psychology* (33:5), pp. 1012–1031.
- Sagioglou, C., and Greitemeyer, T. 2014. "Facebook's Emotional Consequences: Why Facebook Causes a Decrease in Mood and Why People Still Use It," *Computers in Human Behavior* (35), Elsevier Ltd, pp. 359–363.
- Saldaña, J. 2015. *The Coding Manual for Qualitative Researchers*, (second ed.), Sage Publications.
- Salleh, N., Hussein, R., Mohamed, N., and Aditiawarman, U. 2013. "An Empirical Study of the Factors Influencing Information Disclosure Behaviour in Social Networking Sites," in *Proceedings of the International Conference on Advanced Computer Science Applications and Technologies*, pp. 181–185.
- Sarathy, R., and Li, H. 2007. "Understanding Online Information Disclosure as a Privacy Calculus Adjusted by Exchange Fairness," in *Proceedings of the 28th International Conference on Information Systems*.
- Sarstedt, M., Henseler, J., and Ringle, C. M. 2011. "Multigroup Analysis in Partial Least Squares (PLS) Path Modeling: Alternative Methods and Empirical Result," *Advances in International Marketing* (22:11), pp. 195–218.
- Sasaki, Y., Kawai, D., and Kitamura, S. 2016. "Unfriend or Ignore Tweets?: A Time Series Analysis on Japanese Twitter Users Suffering from Information Overload," *Computers in Human Behavior* (64), Elsevier Ltd, pp. 914–922.
- Savitsky, K., Epley, N., and Gilovich, T. 2001. "Do Others Judge Us as Harshly as We Think? Overestimating the Impact of Our Failures, Shortcomings, and Mishaps," *Journal of Personality and Social Psychology* (81:1), pp. 44–56.

- Savitsky, K., Keysar, B., Epley, N., Carter, T., and Swanson, A. 2011. "The Closeness-Communication Bias: Increased Egocentrism Among Friends Versus Strangers," *Journal of Experimental Social Psychology* (47:1), pp. 129–273.
- Schau, H. J., and Gilly, M. C. 2003. "We Are What We Post? Self- Presentation in Personal Web Space.," *Journal of Consumer Research* (30:3), pp. 385–404.
- Schlenker, B. R. 1975. "Self-Presentation: Managing the Impression of Consistency When Reality Interferes with Self-Enhancement.," *Journal of Personality and Social Psychology* (32:6), pp. 1030–1037.
- Schlenker, B. R., and Leary, M. R. 1982. "Audiences' Reactions to Self-Enhancing, Self-Denigrating, and Accurate Self-Presentations," *Journal of Experimental Social Psychology* (18:1), pp. 89–104.
- Schomakers, E. M., Lidynia, C., Müllmann, D., and Ziefle, M. 2019. "Internet Users' Perceptions of Information Sensitivity – Insights from Germany," *International Journal of Information Management* (46), Elsevier Ltd, pp. 142–150.
- Schrammel, J., Köffel, Chritina, and Tscheligi, M. 2009a. "How Much Do You Tell?: Information Disclosure Behaviour Indifferent Types of Online Communities," *Proceedings of the Fourth International Conference on Communities and Technologies*, pp. 275–284.
- Schrammel, J., Köffel, Christina, and Tscheligi, M. 2009b. "Personality Traits, Usage Patterns and Information Disclosure in Online Communities," *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology*, pp. 169–174.
- Schreiner, M., and Hess, T. 2015. "Why Are Consumers Willing to Pay for Privacy? An Application of the Privacy-Freemium Model to Media Companies," in *Proceedings of the 23rd European Conference on Information Systems*.
- Schriesheim, C., Powers, K., Scandura, T., Gardiner, C., and Lankall, M. 1993. "Improving Construct Measurement n Management Research: Comments and a Quantitative Approach for Assessing the Theoretical Content Adequacy of Paper-and-Pencil Survey-Type Instruments," *Journal of Management* (19:2), pp. 385–417.
- Schröder-Abé, M., and Schütz, A. 2011. "Walking in Each Other's Shoes: Perspective Taking Mediates Effects of Emotional Intelligence on Relationship Quality," *European Journal of Personality* (25), pp. 155–169.
- Schudy, S., and Utikal, V. 2017. "'You Must Not Know About Me' - On the Willingness to Share Personal Data," *Journal of Economic Behavior and Organization* (141), Elsevier B.V., pp. 1–13.
- Schweitzer, M. E., and Hsee, C. K. 2002. "Stretching the Truth: Elastic Justification and Motivated Communication of Uncertain Information," *The Journal of Risk and Uncertainty* (25:2), pp. 185–201.
- Scopelliti, I., Loewenstein, G., and Vosgerau, J. 2015. "You Call It 'Self-Exuberance'; I Call It 'Bragging': Miscalibrated Predictions of Emotional Responses to Self-Promotion," *Psychological Science*, pp. 1–12.
- Scott, G. G., and Ravenscroft, K. 2017. "Bragging on Facebook: The Interaction of Content Source and Focus in Online Impression Formation," *Cyberpsychology, Behavior, and Social Networking* (20:1), pp. 58–63.
- Seiders, K., and Berry, L. L. 1998. "Service Fairness: What It Is and Why It Matters," *The Academy of Management Executive* (1993-2005) (12:2), pp. 8–20.

- Sharma, S., and Crossler, R. E. 2014. "Disclosing Too Much? Situational Factors Affecting Information Disclosure in Social Commerce Environment," *Electronic Commerce Research and Applications* (13:5), Elsevier, pp. 305–319.
- Sheng, H., Nah, F. F.-H., and Siau, K. 2008. "An Experimental Study on U-Commerce Adoption: Impact of Personalization and Privacy Concerns," *Journal of the Association for Information Systems* (9:6), pp. 344–376.
- Shibchurn, J., and Yan, X. 2015a. "Information Disclosure on Social Networking Sites: An Intrinsic-Extrinsic Motivation Perspective," *Computers in Human Behavior* (44), pp. 103–117.
- Shibchurn, J., and Yan, X. 2015b. "Information Disclosure on Social Networking Sites: An Intrinsic-Extrinsic Motivation Perspective," *Computers in Human Behavior* (44), pp. 103–117.
- Sierra, J. J., and McQuitty, S. 2005. "Service Providers and Customers: Social Exchange Theory and Service Loyalty," *Journal of Services Marketing* (19:6), pp. 392–400.
- Singleton, S., and Harper, J. 2001. "With a Grain of Salt - What Consumer Privacy Surveys Don't Tell Us," *Competitive Enterprise Institute*.
- Sleeper, M., Balebako, R., Das, S., McConahy, A. L., Wiese, J., and Cranor, L. F. 2013. "The Post That Wasn't: Exploring Self-Censorship on Facebook," in *Proceedings of the Conference on Computer Supported Cooperative Work* (Vol. 13).
- Smith, A. 2014. "Half of Online Americans Don't Know What a Privacy Policy Is." (<http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/>).
- Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989–1016.
- Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly: Management Information Systems* (20:2), pp. 167–195.
- Solomon, M. R., Bamossy, G. J., Askegaard, S. T. A., and Hogg, M. K. 2006. *Consumer Behaviour: A European Perspective*, Financial Times/Prentice Hall.
- Son, J.-Y., and Kim, S. S. 2008. "Internet User's Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly* (32:3), pp. 503–529.
- Spataro, J. 2020. "Remote Work Trend Report: Meetings," *Microsoft*. (<https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/09/remote-work-trend-report-meetings/>).
- Spiekermann, S., Acquisti, A., Böhme, R., and Hui, K. 2015a. "The Challenges of Personal Data Markets and Privacy," *Electronic Markets* (25:1), pp. 161–167.
- Spiekermann, S., Böhme, R., Acquisti, A., and Hui, K. L. 2015b. "Personal Data Markets," *Electronic Markets* (25:2), Springer Verlag, pp. 91–93.
- Spiekermann, S., and Korunovska, J. 2017. "Towards A Value Theory for Personal Data," *Journal of Information Technology* (32:1), pp. 62–84.
- Spiekermann, S., Korunovska, J., and Bauer, C. 2012. "Psychology Of Ownership And Asset Defense: Why People Value Their Personal Information Beyond Privacy," in *Proceedings of the 33rd International Conference on Information Systems*.

- Strull, T. K., and Wyer, R. S. 1988. *Advances in Social Cognition*, (Hillsdale, ed.), Lawrence Erlbaum.
- Staddon, J., Huffaker, D., Brown, L., and Sedley, A. 2012. "Are Privacy Concerns a Turn-off? Engagement and Privacy in Social Networks," in *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12*, New York, USA: ACM Press.
- Staiano, J., Oliver, N., Lepri, B., Oliveira, R. De, Caraviello, M., and Sebe, N. 2014. "Money Walks: A Human-Centric Study on the Economics of Personal Mobile Data," in *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*.
- Statista. 2014a. "Distribution of Global Internet Users Who Say They Are Online at Least 10 Times a Day as of July 2014, by Gender." (<https://www.statista.com/statistics/408674/global-continuously-connected-internet-users-gender/>, accessed April, 2018).
- Statista. 2014b. "Internet Users by Age Worldwide." (<https://www.statista.com/statistics/272365/age-distribution-of-internet-users-worldwide/>).
- Statista. 2017a. "Distribution of Facebook Users Worldwide as of January 2017, by Age and Gender." (<https://www.statista.com/statistics/376128/facebook-global-user-age-distribution/>, accessed April, 2018).
- Statista. 2017b. "Most Famous Social Network Sites Worldwide as of September 2017, Ranked by Number of Active Users (in Millions)." (<https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>, accessed April 2018).
- Statista. 2018a. "Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2018." (<https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>, accessed April, 2018).
- Statista. 2018b. "Most Popular Apple App Store Categories in January 2018." (<https://www.statista.com/statistics/270291/popular-categories-in-the-app-store/>, accessed June 2, 2018).
- Statista. 2020a. "Daily Active Users of Instagram Stories 2019." (<https://www.statista.com/statistics/730315/instagram-stories-dau/>, accessed August 12, 2020).
- Statista. 2020b. "Since the Cambridge Analytica Affair, Are You Planning on Deleting Your Facebook Account Soon?" (<https://www.statista.com/statistics/1094463/cambridge-analytica-willingness-to-unsubscribe-from-facebook-france/>, accessed August 12, 2020).
- Statista. 2020c. "Facebook's Average Revenue Per User (ARPU) From 2012 to 2019." (<https://www.statista.com/statistics/234056/facebooks-average-advertising-revenue-per-user/>, accessed November 16, 2020).
- Steinfeld, N. 2015. "Trading with Privacy: The Price of Personal Information," *Online Information Review* (39:7), pp. 923–938.
- Stern, T., and Salb, D. 2015. "Examining Online Social Network Use and Its Effect on the Use of Privacy Settings and Profile Disclosure," *Bulletin of Science, Technology & Society* (35:1–2), pp. 25–34.
- Stutzman, F., Capra, R., and Thompson, J. 2011. "Factors Mediating Disclosure in Social Network Sites," *Computers in Human Behavior* (27:1), pp. 590–598.

- Sutanto, J., Palme, E., and Tan, C. 2014. "Addressing the Personalization–Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users," *Management Information Systems Quarterly* (37:4), pp. 1141–1164.
- SYZGY. 2018. "The Price of Personal Data: How Much Do People Believe Their Data Is Worth?," SYZGY Digital Insight Survey 2018."
- Tamir, D. I., and Mitchell, J. P. 2012. "Disclosing Information about the Self Is Intrinsically Rewarding," *Proceedings of the National Academy of Sciences* (109:21), pp. 8038–8043.
- Tandoc, E. C., Ferrucci, P., and Duffy, M. 2015. "Facebook Use, Envy, and Depression Among College Students: Is Facebooking Depressing?," *Computers in Human Behavior* (43), Elsevier Ltd, pp. 139–146.
- Taylor, D. A., and Altman, I. 1975. "Self-Disclosure as a Function of Reward-Cost Outcomes," *Sociometry* (38:1), pp. 18–31.
- Tidwell, L. C., and Walther, J. B. 2002. "Computer-Mediated Communication Effects on Self-Disclosure, Impressions, and Interpersonal Evaluations," *Human Communication Research* (28:3), pp. 317–348.
- Trepte, S., Scharkow, M., and Dienlin, T. 2020. "The Privacy Calculus Contextualized: The Influence of Affordances," *Computers in Human Behavior* (104), Elsevier Ltd.
- Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., and Lind, F. 2015. "Do People Know About Privacy and Data Protection Strategies? Towards the 'Online Privacy Literacy Scale' (OPLIS)," in *Reforming European Data Protection Law*, Dordrecht: Springer, pp. 333–365.
- Tsai, J. Y., Egelman, S., Cranor, L., and Acquisti, A. 2011. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research* (22:2), pp. 254–268.
- Tufekci, Z. 2007. "Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites," *Bulletin of Science, Technology & Society* (28:1), pp. 20–36.
- Turel, O. 2015. "Quitting the Use of a Habituated Hedonic Information System: A Theoretical Model and Empirical Examination of Facebook Users," *European Journal of Information System* (4:24), pp. 431–446.
- Turel, O., Yuan, Y., and Connelly, C. E. 2008. "In Justice We Trust: Predicting User Acceptance of E-Customer Services," *Journal of Management Information Systems* (24:4), Routledge, pp. 123–151.
- Tversky, A., and Kahneman, D. 1973. "Judgment Under Uncertainty: Heuristics and Biases," *Science* (185), pp. 1124–1131.
- Tzortzaki, E., Kitsiou, A., Sideri, M., and Gritzalis, S. 2016. "Self-Disclosure , Privacy Concerns and Social Capital Benefits Interaction in FB: A Case Study," in *Proceedings of the 20th Pan-Hellenic Conference on Informatics*.
- Udo, G. J., Bagchi, K. K., and Kirs, P. J. 2010. "An Assessment of Customers' E-Service Quality Perception, Satisfaction and Intention," *International Journal of Information Management* (30:6), Elsevier Ltd, pp. 481–492.
- Utz, S. 2015. "The Function of Self-Disclosure on Social Network Sites: Not Only Intimate, but Also Positive and Entertaining Self-Disclosures Increase the Feeling of Connection," *Computers in Human Behavior* (45), Elsevier Ltd, pp. 1–10.

- Utz, S., Tanis, M., and Vermeulen, I. 2012. "It Is All About Being Popular: The Effects of Need for Popularity on Social Network Site Use," *Cyberpsychology, Behavior, and Social Networking* (15:1), pp. 37–42.
- Valenzuela, S., Park, N., and Kee, K. F. 2009. "Is There Social Capital in a Social Network Site?: Facebook Use and College Student's Life Satisfaction, Trust, and Participation," *Journal of Computer-Mediated Communication* (14:4), pp. 875–901.
- Venkatesh, V., Brown, S. A., and Bala, H. 2013. "Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems," *MIS Quarterly* (37:1), pp. 21–54.
- Vetter, J., Benlian, A., and Hess, T. 2011. "Overconfidence in IT Investment Decisions: Why Knowledge Can Be a Boon and Bane at the Same Time," in *Proceedings of the International Conference on Information Systems*.
- Vogel, E. A., Rose, J. P., Roberts, L. R., and Eckles, K. 2014. "Social Comparison, Social Media, and Self-Esteem," *Psychology of Popular Media Culture* (3:4), pp. 206–222.
- Voss, K. E., Spangenberg, E. R., and Grohmann, B. 2003. "Measuring the Hedonic and Utilitarian Dimensions of Consumer Attitude," *Journal of Marketing Research* (40:3), pp. 310–320.
- Wagner, A., Abramova, O., Krasnova, H., and Buxmann, P. 2018b. "When You Share, You Should Care: Examining The Role of Perspective-Taking on Social Networking Sites," in *Proceedings of the European Conference on Information Systems*.
- Wagner, A., Abramova, O., Krasnova, H., Buxmann, P., and Benbasat, I. 2018c. "From 'Privacy Calculus' to 'Social Calculus': Understanding Self-Disclosure on Social Networking Sites," in *Proceedings of the 39th International Conference on Information Systems*.
- Wagner, A., Olt, C. M., and Abramova, O. 2021. "Calculating versus Herding in the Adoption of a Privacy-Invasive Information System: The Case of COVID-19 Tracing Apps," in *Proceedings of the European Conference on Information Systems*.
- Wagner, A., Wessels, N., Buxmann, P., and Krasnova, H. 2018a. "Putting a Price Tag on Personal Information - A Literature Review," in *Proceedings of the 51st Hawaii International Conference on System Sciences*.
- Wakefield, R. 2013. "The Influence of User Affect in Online Information Disclosure," *Journal of Strategic Information Systems* (22:2), Elsevier B.V., pp. 157–174.
- Walther, J. B. 1996. "Computer-Mediated Communication: Impersonal, Interpersonal, and Hyperpersonal Interaction," *Communication Research* (23:1), pp. 3–43.
- Walther, J. B. 2007. "Selective Self-Presentation in Computer-Mediated Communication: Hyperpersonal Dimensions of Technology, Language, and Cognition," *Computers in Human Behavior* (23:5), pp. 2538–2557.
- Wang, J., Li, Y., and Rao, H. R. 2016. "Overconfidence in Phishing Email Detection," *Journal of the Association for Information Systems* (17:11), pp. 759–783.
- Wang, S. S., and Stefanone, M. A. 2013. "Showing Off? Human Mobility and the Interplay of Traits, Self-Disclosure, and Facebook Check-Ins," *Social Science Computer Review* (31:4), pp. 437–457.

- Wang, T., Duong, T. D., and Chen, C. C. 2016. "Intention to Disclose Personal Information via Mobile Applications: A Privacy Calculus Perspective," *International Journal of Information Management* (36:4), Elsevier Ltd, pp. 531–542.
- Warren, S. D., and Brandeis, L. D. 1890. "The Right to Privacy," *Harvard Law Review* (4:5), pp. 193–220.
- Watson, D., and Clark, L. A. 1999. "The PANAS-X: Manual for the Positive and Negative Affect Schedule - Expanded Form," *Iowa Research Online*.
- Webster, J., and Watson, R. T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly* (26:2), xiii–xxiii.
- Weinstein, N. 1980. "Unrealistic Optimism About Future Life Events," *Journal of Personality and Social Psychology* (39:5), pp. 806–820.
- Wenninger, H., Lee, Z. W. Y., Cheung, C. M. K., Chan, T. K. H., and Wong, R. Y. M. 2016. "A Literature Analysis About Social Information Contribution and Consumption on Social Networking Sites," in *Proceedings of the European Conference on Information Systems*.
- Westin, A. F. 1991. *Equifax-Harris Consumer Privacy Survey*, New York: Louis Harris & Associates: Equifax, Inc.
- Westley, B. H., and MacLean Jr, M. S. 1957. "A Conceptual Model for Communication Research," *Journalism Quarterly* (34), pp. 31–38.
- Wheeless, L. R., and Grotz, J. 1976. "Conceptualization and Measurement of Reported Self-Disclosure," *Human Communication Research* (2:4), pp. 338–346.
- White, J. M. 1985. "Perceived Similarity and Understanding in Married Couples," *Journal of Social and Personal Relationships* (2:1), pp. 45–57.
- Wibson. 2019. "Don't Give Away Your Data for Free. Make a Profit." (<https://wibson.org/>).
- Wilson, D., and Valacich, J. 2012. "Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus," in *Proceedings of the International Conference on Information Systems*.
- Wirth, J., Maier, C., and Laumer, S. 2019. "Subjective Norm and the Privacy Calculus: Explaining Self-Disclosure on Social Networking Sites," in *Proceedings of the 27th European Conference on Information Systems*.
- Wunderman Thompson. 2020. "Trend Report: The Privacy Era," New York. (<https://www.wundermanthompson.com/insight/the-data-privacy-and-security-report>).
- Xia, L., Monroe, K. B., and Cox, J. L. 2012. "The Price Is Unfair ! A of Price Framework Fairness," *Journal of Marketing* (68:4), pp. 1–15.
- Xie, W., and Kang, C. 2015. "See You, See Me: Teenagers' Self-Disclosure and Regret of Posting on Social Network Site," *Computers in Human Behavior* (52), Elsevier Ltd, pp. 398–407.
- Xu, H., Dinev, T., Smith, H. J., and Hart, P. 2008. "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View," in *Proceedings of International Conference on Information Systems*.
- Xu, H., Dinev, T., Smith, J., and Hart, P. 2011a. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems* (12:12), pp. 789–824.

- Xu, H., and Gupta, S. 2009. "The Effects of Privacy Concerns and Personal Innovativeness on Potential and Experienced Customers' Adoption of Location-Based Services," *Electronic Markets* (19:2-3), pp. 137-149.
- Xu, H., Hock-Hai, T., Tan, B. C. Y., and Agarwal, R. 2012. "Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services," *Information Systems Research* (23:4), pp. 1342-1363.
- Xu, H., Luo, X., Carroll, J. M., and Rosson, M. B. 2011b. "The Personalization Privacy Paradox: An Exploratory Study of Decision Making Process for Location-Aware Marketing," *Decision Support Systems* (51:1), pp. 42-52.
- Xu, H., Teo, H.-H., Tan, B. C. Y., and Agarwal, R. 2009. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3), pp. 135-174.
- Xu, H., and Teo, H. 2004. "Alleviating Consumers' Privacy Concerns in Location-Based Services: A Psychological Control Perspective," in *Proceedings of the International Conference on Information Systems*.
- Xu, H., Teo, H., and Tan, B. C. Y. 2005. "Predicting the Adoption of Location-Based Services: The Role of Trust and Perceived Privacy Risk," in *Proceedings of the International Conference on Information Systems*.
- Yao, G., Wu, C. H., and Yang, C. T. 2008. "Examining the Content Validity of the WHOQOL-BREF from Respondents' Perspective by Quantitative Methods," *Social Indicators Research* (85:3), pp. 483-498.
- Yieh, K., Chiao, Y. C., and Chiu, Y. K. 2007. "Understanding the Antecedents to Customer Loyalty by Applying Structural Equation Modeling," *Total Quality Management and Business Excellence* (18:3), pp. 267-284.
- Yu, J., Hu, P. J.-H., and Cheng, T.-H. 2015. "Role of Affect in Self-Disclosure on Social Network Websites: A Test of Two Competing Models," *Journal of Management Information Systems* (32:2), pp. 239-277.
- Yu, L., and Wu, M. 2010. "The Relation of Personality and Self-Disclosure on Renren," in *Proceedings of the 2nd Symposium on Web Society*, pp. 435-442.
- Zeng, X., and Wei, L. 2013. "Social Ties and User Content Generation: Evidence from Flickr," *Information Systems Research Publication* (24:1), pp. 71-87.
- Zephora. 2015. "The Top 20 Valuable Facebook Statistics - Updated November 2017." (<https://zephoria.com/top-15-valuable-facebook-statistics/>, accessed April, 2018).
- Zhang, Y., and Ling, Q. 2015. "SNS as Intimacy Zone: Social Intimacy, Loneliness, and Self-Disclosure on SNS," *Global Media Journal* (13:25).
- Zhao, C., Street, D. L., and Hinds, P. 2012. "How and to Whom People Share: The Role of Culture in Self-Disclosure in Online Communities," *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work*, pp. 67-76.
- Zhao, L., Lu, Y., and Gupta, S. 2012. "Disclosure Intention of Location-Related Information in Location-Based Social Network Services," *International Journal of Electronic Commerce* (16:4), pp. 53-90.

- Zhao, S., Grasmuck, S., and Martin, J. 2008. "Identity Construction on Facebook: Digital Empowerment in Anchored Relationships," *Computers in Human Behavior* (24:5), pp. 1816–1836.
- Zhu, Y., and Chen, H. 2012. "Service Fairness and Customer Satisfaction in Internet Banking: Exploring the Mediating Effects of Trust and Customer Value," *Internet Research* (22:4), Emerald, pp. 482–498.
- Zlatolas, L. N., Welzer, T., Hericko, M., and Hölbl, M. 2015. "Privacy Antecedents for SNS Self-Disclosure: The Case of Facebook," *Computers in Human Behavior* (45), pp. 158–167.

Appendix

Appendix 1. Distributive Equity Measurements in the IS Field (Paper 1.C).

Reference	Study Design	Context	Theoretical Foundation	Operationalization of Distributive Equity	Key Consequence(s) of Distributive Equity	Comment
Krasnova et al. 2010 (self-developed, inspired by Son and Kim 2008)	Online survey of N = 237 students (73.4%) based in Germany	Social Networking Sites	Justice Theory	How fair is the following? 1. I would find it fair that some of the profile information I provide can be used for personalized advertising in exchange for free social networking services. 2. The benefits I receive from OSN are attractive enough to let OSN use some of my profile information for marketing purposes. 3. The fact that some of my profile information can be used for commercial purposes could be compensated by benefits I receive from OSN. Distributive Justice (seven-point scales anchored with "strongly disagree" and "strongly agree") 1. Online companies that have my personal information provide better value than those without holding my personal information. 2. The level of service from online companies that use my personal information is superior to the service from companies that do not use my personal information. 3. What I give up in terms of releasing my personal information to online companies is commensurate with what I receive in return from the companies. 4. Given the potential problem of releasing my personal information to online companies, the benefits I receive from the companies are fair.	(Trust) (Privacy Concerns)	Call for research to further investigate distributive equity judgements and its outcomes.
Son and Kim 2008 (self-developed)	Online survey of N = 523 internet users based in the U.S.	Online companies in general	Information Privacy, Justice Theory	Distributive Justice (seven-point Likert scale: "to a small extent"/"to a large extent") 1. Does your outcome reflect the effort you put into resolving the complaint? 2. Is your outcome appropriate for the process you have completed? 3. Is your outcome similar to your expectations of it? 4. Is your outcome justified, given the case details?	Perceived Justice + Refusal - Misrepresentation -	Distributive Fairness was operationalized as a balancing act between benefits and risks of information disclosure.
Turel et al. 2008 (adapted from Colquitt et al. 2001)	Online experiment of N = 380 (nested dyads) students based in the U.S.	prototypical eBay complaint cases	Trust Theory, Justice Theory	Distributive Justice (seven-point scales anchored with "strongly disagree" and "strongly agree") 1. The service level of this service provider is superior to that of the service providers that do not use my personal information. 2. This mobile service provider presents better values than the service providers that do not have my personal information. 3. What I give up in terms of disclosing my personal information to the service provider is commensurate with what I acquire from it. 4. Given the potential problems derived from disclosing my personal information to the service provider, the benefits I acquire are fair.	Trust in Service Representative + Trust in E-Customer-Service + (Intention to re-use Service)	Distributive Fairness was operationalized as users' balancing act between input in terms of effort and outcomes in terms of complaint handling.
Zhou 2011 (adapted from Son and Kim 2008)	Survey of N = 245 mobile users based in China	Location-based services	Justice Theory		Continuous usage intention + Privacy Risk - Perceived usefulness +	Distributive Fairness was operationalized as a balancing act between benefits and risks of information disclosure.

Appendix 2. Overview of Construct Measurements and Item Loadings (Paper 1.C).

Construct	Item Code	Item	Item Loading
Users' Net Value (UNV)	UNV1	I think the benefits that Facebook brings me outweighs my privacy risks.	.892
	UNV2	The benefits associated with using Facebook are attractive enough compared to the privacy risks that come with it.	.924
	UNV3	Facebook is more beneficial to me than it poses a privacy risk to me.	.883
Information Sensitivity (IS)	IS1	My Facebook profile is...	.898
	IS2	My personal information collected by Facebook is...	.919
	IS3	My information disclosed to Facebook is...	.880
Distributive Equity (DE)	DF1	What I receive from using the services of the company is fair with regard to their profit.	.931
	DF2	The ratio between what I get out of using the service provided by the company and the profit the firm makes with me is fair.	.935
	DF3	I think what the company earns with me is fair in comparison to what they offer me.	.954
	DF4	The service the company offers me is commensurate with what they earn with it.	.922
	DF5	The profit the company makes is fair, given the service I receive.	.950
Satisfaction (SAT)	SAT1	I am very satisfied.	.913
	SAT2	I am very pleased.	.931
	SAT3	I am very contented.	.939
	SAT4	I am very delighted.	.915
Continuance Intention (CI)	CI1	In the near future, I intend to continue using Facebook.	.966
	CI2	I intend to continue using Facebook.	.977
	CI3	I predict that I would continue using Facebook.	.972

[illegible]

Appendix 4. Survey Items (Paper 2.A).

Perceived Risk of Information Disclosure - (Malhotra et al. 2004)			
7 pt. Likert Scale anchored with “strongly disagree” and “strongly agree”			
RSK1	In general, it would be risky to disclose my personal information to this application.		
RSK2	There would be high potential for loss associated with providing my personal information to this application.		
RSK3	There would be too much uncertainty associated with having my personal information gathered by this application.		
RSK4	Providing the provider of the application with my personal information would involve many unexpected problems.		
RSK5	I would feel safe giving my personal information to the provider of this application. (reverse)		
Hedonic (HED) and Utilitarian (UTL) Attitudes towards the Application - (Voss et al. 2003)			
7 pt. semantic differentials			
HED1	Not fun / Fun	UTL1	Ineffective / Effective
HED2	Dull / Exciting	UTL2	Unhelpful / Helpful
HED3	Not delightful / Delightful	UTL3	Not functional / Functional
HED4	Not thrilling / Thrilling	UTL4	Unnecessary / Necessary
HED5	Unenjoyable / Enjoyable	UTL5	Impractical / Practical
Intention to use the Application - (Malhotra et al. 2004)		Visual Appeal of App Logo - (based on Montoya-Weiss et al. 2003)	
To what extent would you download this application to give it a try? (1 – 7)		7 pt. semantic differentials	
INT1	Unlikely / Likely	VIS1	I like the look of the logo.
INT2	Not probable / Probable	VIS2	The logo is attractive to me.
INT3	Impossible / Possible	VIS2	I like the graphics of the logo.
INT4	Unwilling / Willing		
Perceived Evaluability of Privacy Risks (self-developed)			
7pt Likert Scale anchored with “strongly disagree” and “strongly agree” While rating the privacy risks...			
EVA1	... I had sufficient information at hand.	EVA4	... I was able to decide by instinct.
EVA2	... I had a good judgment.	EVA5	... I knew exactly how I would answer.
EVA3	... it was easy for me to tick the checkboxes.		

Appendix 5. Descriptive Statistics of Constructs in the Research Model (Paper 2.A).

			Perceived Risk		Hedonic Attitude		Utilitarian Attitude		Behavioral Intention	
	App	N	Mean	SD	Mean	SD	Mean	SD	Mean	SD
Single Evaluation	A	63	3.95	1.41	2.89	1.18	4.70	1.16	4.04	1.76
	B	67	4.32	1.28	3.39	1.10	4.95	1.15	4.35	1.71
Joint Evaluation	A	103	3.27	1.35	3.12	1.14	4.90	1.14	4.71	1.40
	B	103	4.78	1.32	4.02	1.17	4.76	1.16	3.68	1.66

Appendix 6. Privacy Quiz (F=false; T=true) (Paper 2.B).

Q1	Most mobile apps, such as Facebook or Google Maps, monitor and store the behavior of their users. (T)
Q2	If a mobile app contains a privacy policy, this means that the app will not share its user information with other companies. (F)
Q3	The EU Data Protection Directive limits how long user data may be stored. (F)
Q4	Many apps require access rights to information such as contacts, calendars, etc. of their users, although this information would not be necessary for the core functionalities of the app. (T)
Q5	The same standard terms and conditions apply to all social networking sites. Deviations must be indicated by the operators. (F)
Q6	Social network operators (e.g., Facebook) also collect and process information from people who do not use their network at all. (T)
Q7	If you own a smartphone, you give government agencies the ability to track your location. (T)
Q8	Many apps access user information, such as their location, even when the app is not in use. (T)
Q9	Each Messenger app uses end-to-end encryption. (F)
Q10	Paid apps offer higher data protection. (F)